ULTRALOG

Survivable Logistics Information Systems

Dr. Mark Greaves
703-526-6623
mgreaves@darpa.mil

September 2002

UltraLog Goals

Two Core Challenges for Transformation

- **End-to-end control of the entire logistics pipeline**
  - Simultaneous planning and execution
  - Operating at all echelons and during all phases of the operation
  - Interoperable over highly distributed organizations
- **Survivability of information systems in a harsh wartime environment**
  - Environmental Dynamism: Security will fail, machines will fail or be destroyed, bugs will happen, the environment will change at high velocity
  - Multiple Simultaneous Threats: Information warriors will target our software; kinetic warriors will target our hardware
  - System Complexity: Coalition operations, deep supply chains, and other modern teaming and trust arrangements create massive interdependencies
    - Systems-of-systems lack the unified architecture and controls typical of traditional fault-tolerant systems approaches
  - Security barriers alone will not result in a survivable system

Transforming the Logistics Infrastructure

Advanced Logistics Project (FY96—FY01)

UltraLog Program (FY01—FY04)

- End-to-End Control of the Logistics Pipeline
  - Fastest ever construction of a level-5 logistics plan (~hour [agents] vs. weeks [humans])
  - Completely distributed agent-based system architecture based around business processes
  - Policy-driven bottom-up demand generation and sourcing
- Hardened and Survivable Logistics
  - Robust, Secure, and Scalable logistics agents
  - Designed to withstand simultaneous cyber and kinetic
    attack with controlled performance degradation
  - Agent technology enables new approaches to logistics systems survivability

Agent technology **allows us to build the massive scale survivable logistics information systems needed to achieve Focused Logistics**

Technology for Transformation

Advanced Logistics Project (FY96—FY01)

- Use agents to build the world’s largest, most complex distributed planning system
  - Achieve an order-of-magnitude reduction in planning time
  - Technology: distributed planning agents as middleware
  - Challenge Problem: 1-hour L5 TPFDD for an SSC, in a lab

UltraLog Program (FY01—FY04)

- Agents^2: Adaptive Survivable Systems
  - Move from a pure planning system to an adaptive, resource-aware, fully distributed execution system
  - Technology: Survivable agents and agent communities
  - Challenge Problem: 1-hour L5 TPFDD for a MRC, and maintain acceptable plan fidelity under kinetic and cyber attack, for a 180 day period including RSOI and operations

Agent technology **will allow us to prove that distributed, adaptive, survivable, massive scale execution systems are possible**

UltraLog

Our enemies can asymmetrically attack us by degrading or denying our logistics information flows

Secure against cyber attack

Robust against damage

Scalable to wartime data loads

Ultralog: Extremely survivable net-centric logistics information systems for the modern battlefield

UltraLog

Problem

Extremely survivable net-centric logistics information systems for the modern battlefield

Secure against cyber attack

Robust against damage

Scalable to wartime data loads

Technical Objectives

Demonstrate agile networks of robust intelligent agents that dynamically balance logistics tasks and system defenses to maximize logistics function while under attack

- Build high-confidence intelligent agents
  - Military-grade security and intrusion response
  - Scalability and fault tolerance designed for wartime environments
- Build adaptive agent societies that function in damaged and stressed environments
  - Controlled degradation with dynamic policies
  - Detect and manage emergent properties
  - Resistant to adversary gaming
- Transition via open architectures and open source

Military Impact

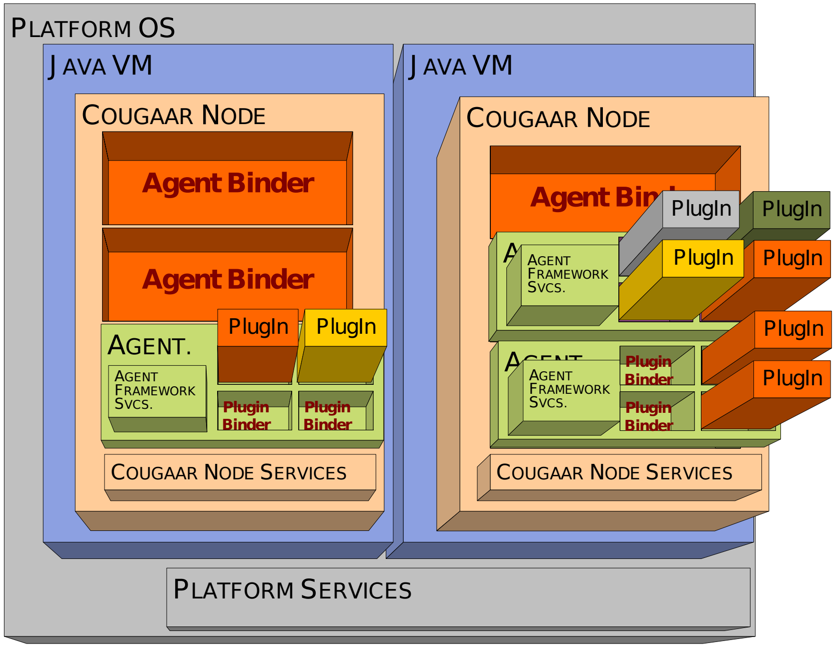
- Secure, scalable, and robust network-centric logistics infra-structure for the modern warfighter
  - Enable precision logistics at high tempos
  - Survivability in the electronic battlefield
- Reliable control of the logistics pipeline
  - Absorb cyber attacks and massive infrastructure loss with controlled degradation and robust failover
  - Scale to multiple operations and global sizes
- A transformational technology for JV2020 Focused Logistics
  - Greater logistics confidence with reduced

Milestones

- Component logistics agent technologies
  - Scalable mobile agent framework Q4/02
  - Security PKI and M&R infrastructure Q1/03
  - Multifailure fault tolerance Q4/03
  - Fully distributed adaptivity engine Q4/03
- Composing agents into societies
  - Single-thread society adaptivity to stress Q1/03
  - Cross-thread society adaptivity to stress Q4/03

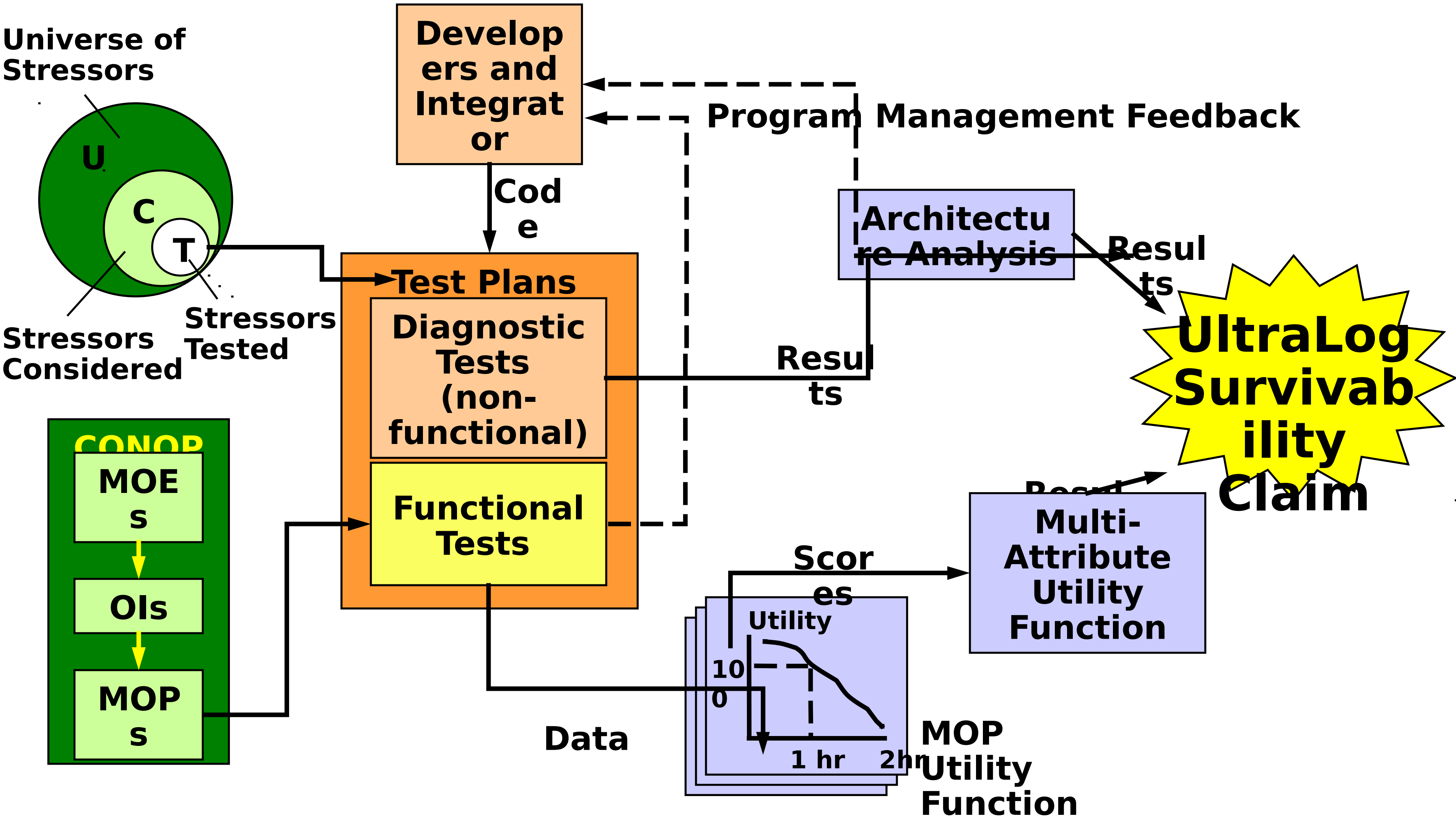
Overall UltraLog Strategy

- **Use Cougaar as a Survivability Laboratory**
  - Agent-based design offers new survivability techniques for large distributed systems
  - Build on logistics domain functionality from the Advanced Logistics Project
- **Implement Mechanisms for Cougaar Security, Scalability, and Robustness**
  - Assume some attacks will get through. Our success at adapting and recovering will define the survivability of our system
  - Control UltraLog society behavior by balancing logistics functionality and system survivability
  - Adapt society task flows to the resources available and the current threat condition
- **Assert and Support a Survivability Claim**
  - Use empirical and analytic means to assess the validity of our survivability claim
  - Develop appropriate metrics and test methods
  - Manage program based on the results of periodic assessments and red team experimentation



Cognitive Agent Architectur (Cougaar) Platform

UltraLog Program Cycle



Universe of Stressors

U

C

T

Stressors Considered

Stressors Tested

CONOP

MOEs

OIs

MOPs

Developers and Integrator

Code

Test Plans

Diagnostic Tests (non-functional)

Functional Tests

Program Management Feedback

Architecture Analysis

Results

Results

UltraLog Survivability Claim

Resul

Multi-Attribute Utility Function

Scores

Utility

100

1 hr

2hr

MOP Utility Function

Data

Requirements Development & Test Analysis Claim

Questions

UltraLog Requirements

UltraLog Preliminaries

Program Framework and Context

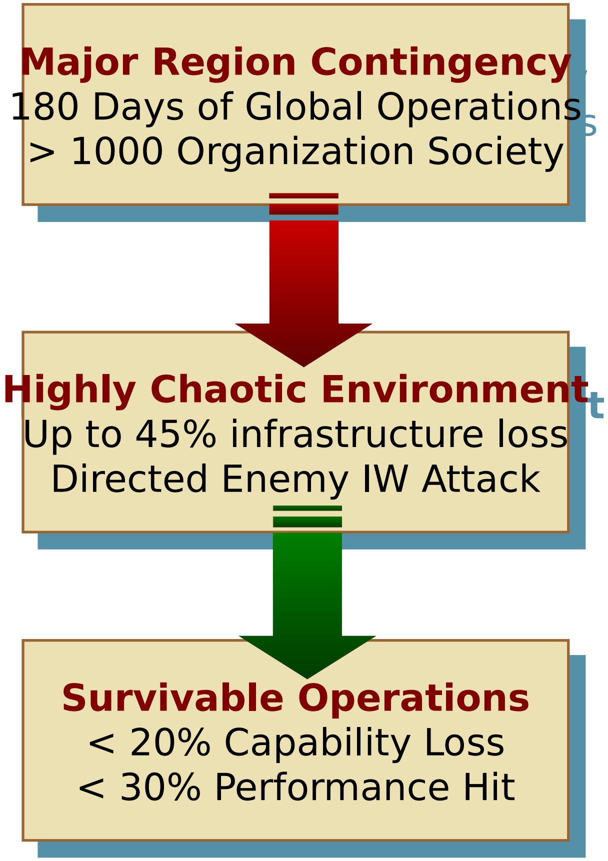
We have a set of designs and strategies that will carry us through the program

- **Architecture for Survivability**
  - Survivability architecture
  - Adaptivity Engine
  - Narratives and requirements
- **Security Approach**
- **Quantitative Framework**
  - MOEs, OIs, MOPs
  - Definitions of key terms, metrics, stressors, approaches
  - Test plans and procedures
  - Multiattribute Utility approach
- **UltraLog Wall Chart**
- **J4-vetted CONOPS**
  - Touchstone for the military employment of UltraLog
  - Motivates requirements and MOPs
- **Turkey / Azerbaijan Scenario**
  - Our reference scenario
  - Can grow and change through the life of the program
- **Integration methods**
  - TIC processes (CVS, JavaDocs…)
  - Separate integration, testing, and assessment teams
  - Test automation with ACME and the UTB

UltraLog Survivability Claim

UltraLog will act to maximally preserve society function under stress, in accordance with policy

- ***Function*** **is defined by requirements**
  - Measures of Effectiveness, Operational Issues, Measures of Performance, Data Requirements, and the MAU score
  - UltraLog has both Logistics MOPs and Security MOPs
- ***Stress*** **is defined by the UltraLog program goals and threat environment**
  - Define Security, Scalability, Robustness stresses
  - Apply stresses singly, per-class, and jointly, in accordance with the experimentation plan
- ***Policy*** **supplies a set of tradeoff constraints**
  - Security policies provide minimum levels of integrity and confidentiality
  - Functional policies constrain the logistics solution
- ***Act to maximally preserve*** **means the generation, optimization, and application of UltraLog control strategies**
  - Define sensors, actuators, state estimators
  - Construct system control laws and strategies



Major Region Contingency
180 Days of Global Operations
> 1000 Organization Society

Highly Chaotic Environment
Up to 45% infrastructure loss
Directed Enemy IW Attack

Survivable Operations
< 20% Capability Loss
< 30% Performance Hit

UltraLog Baseline Requirements

- **MOE 1: Provide a capability to produce executable logistics plan based on the input of a time-phased operations plan, replan for changes in the operations plan and specific external events, and present information to a user**
  - 100% completeness and correctness of the logistics plan elements as determined by installed business rules
  - 100% completeness and completeness of information collected for presentation to a user for selected sets of representative queries
- **MOE 2: Provide a capability to maintain confidentiality and accountability of the logistics plan in accordance with policy**
  - 100% of all sensitive data stored (on the UltraLog blackboards or in UltraLog persistent storage) or in transmission are not available to an unauthorized entity
  - 100% of all user actions are unavailable for invocation by unauthorized users
  - 100% of all designated user actions are recorded
- **MOE 3: Provide sufficient system performance to develop the plan, replan and collect information for presentation to a user in a timely manner**
  - Within one hour, generate a plan upon receipt of an operations plan, or replan upon insertion of a change to the operations plan or specific external events
  - For selected sets of representative queries, collect information for presentation in a timely manner

UltraLog Stressed Requirements

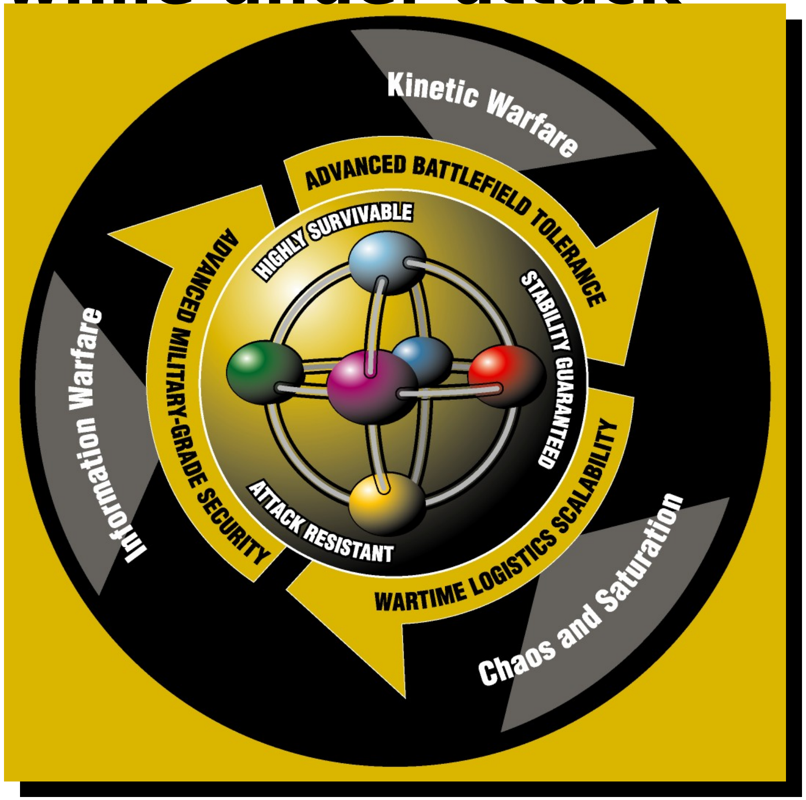
- **MOE 1: Provide a capability to produce executable logistics plan based on the input of a time-phased operations plan, replan for changes in the operations plan and specific external events, and present information to a user**
  - 80% completeness / 95% correctness of the logistics plan elements compared to baseline
  - 80% completeness / 95% correctness of information collected for presentation to a user for selected sets of representative queries
- **MOE 2: Provide a capability to maintain confidentiality and accountability of the logistics plan in accordance with policy**
  - >90% of all sensitive data stored (on the UltraLog blackboards or in UltraLog persistent storage) or in transmission are not available to an unauthorized entity, and that the effort required to disclose 1% of the sensitive data elements has a RTWF cost >$100K
  - >95% of all user actions are unavailable for invocation by unauthorized users, and that the effort required to invoke 1% of unauthorized user actions has a RTWF cost >$100K
  - >95% of all designated user actions designated by policy to be recorded are properly recorded and the effort to prevent the recording of 1% of such designated user actions has a RTWF cost >$100K.
- **MOE 3: Provide sufficient system performance to develop the plan, replan and collect information for presentation to a user in a timely manner**
  - 70% of timing performance as compared to baseline

Questions

UltraLog Technologies

UltraLog Technical Approach

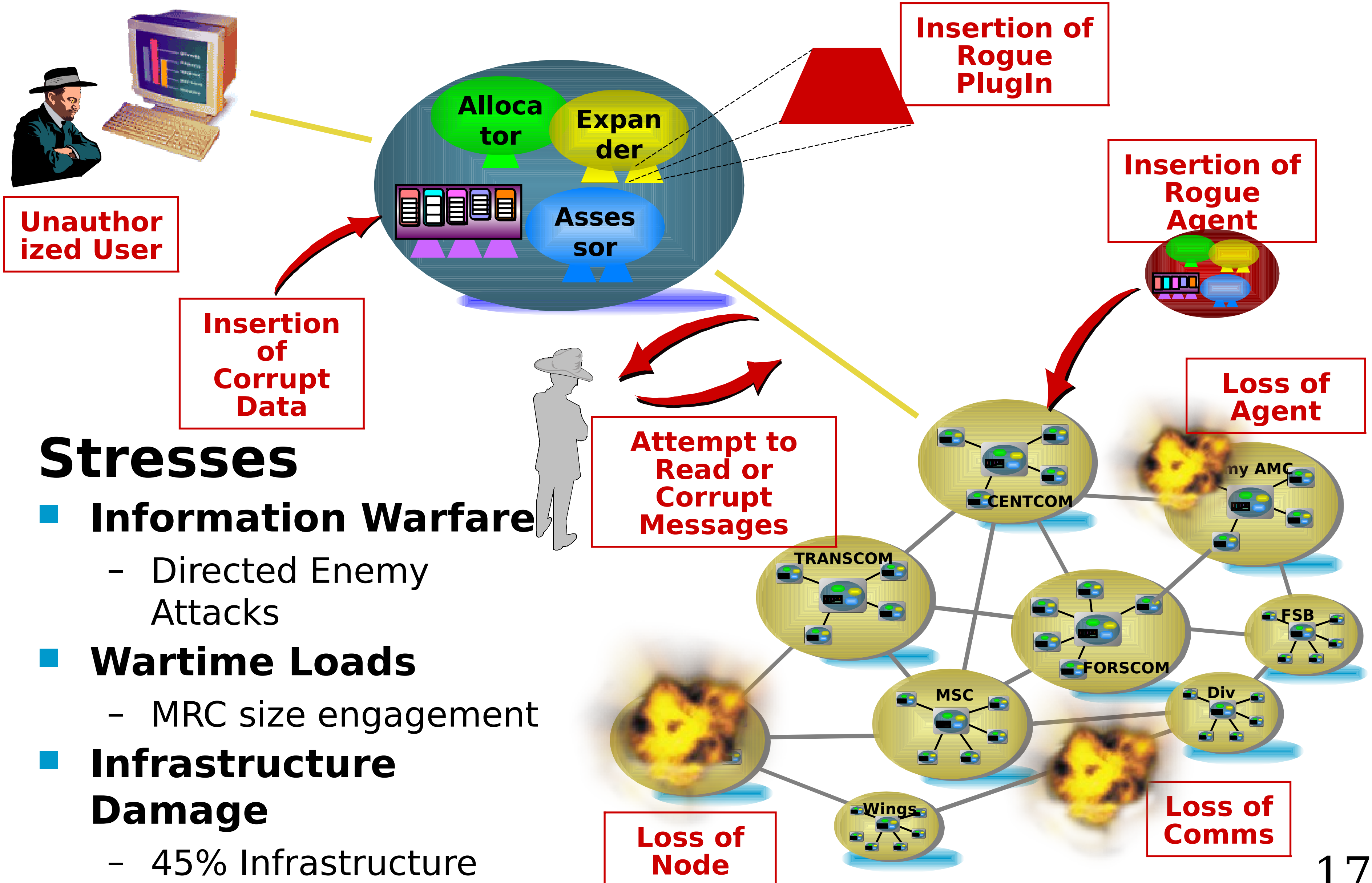
Preserve logistics function while under attack



A survivable logistics information system

- Build high-confidence intelligent agents
  - Military-grade security and intrusion response
  - Scalability and fault tolerance designed for wartime environments
- Build adaptive agent societies that function in damaged and stressed environments
  - Controlled degradation with dynamic policies
  - Detect and manage derivative properties
  - Resistant to adversary gaming
- A network-centric way to achieve higher quality software
  - >500K lines of Java in the controlled core; >900K lines total
  - Open Source adoption

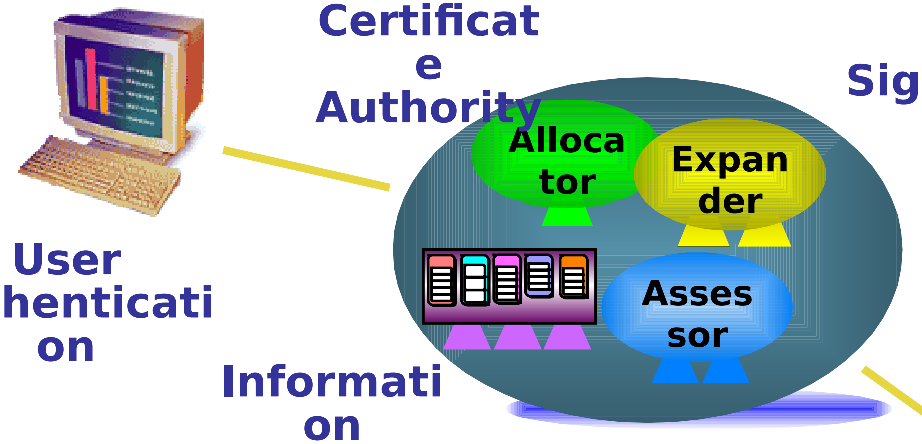
Information System Stresses



Stresses

- **Information Warfare**
  - Directed Enemy Attacks
- **Wartime Loads**
  - MRC size engagement
- **Infrastructure Damage**
  - 45% Infrastructure

Defenses Against Stresses



Certificate Authority

User Authentication

Information Pedigree

Signed JAR Files

Correlation and Verification

Dynamic execution policies based on Threatcon & local conditions

Message Encryption

Adaptivity engines at all levels

DAML Service Directories

Persistence

Running Redundancy

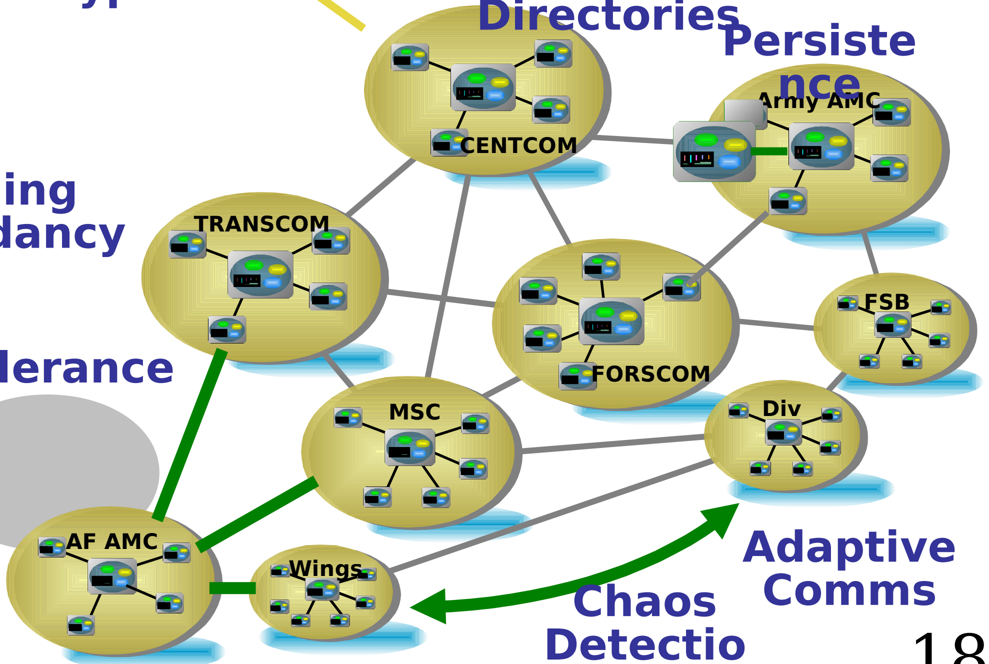
Fault Tolerance

Rehydration

Variable Fidelity Processing

Adaptive Comms

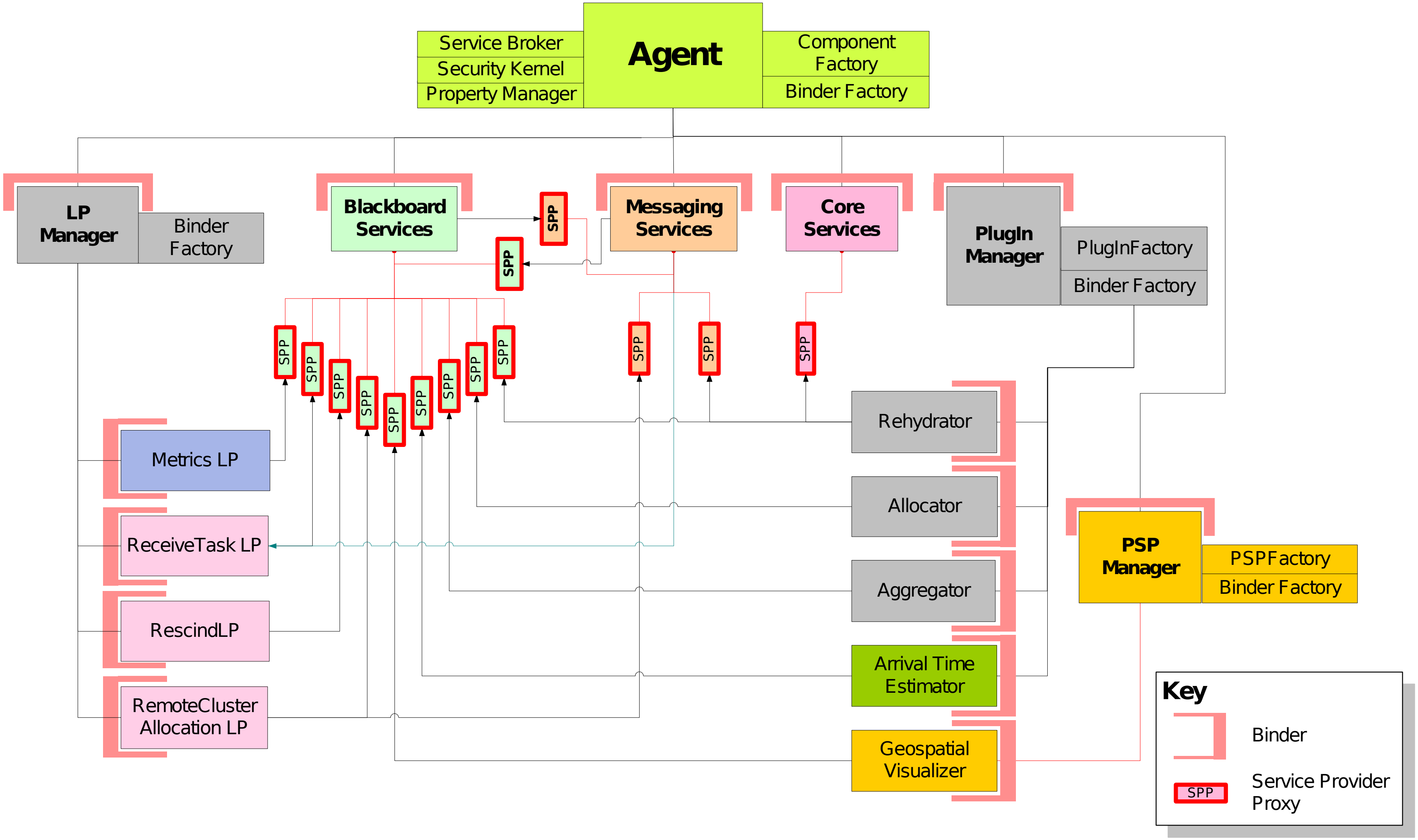
Chaos Detectio



Defenses

- Security
- Scalability
- Robustness

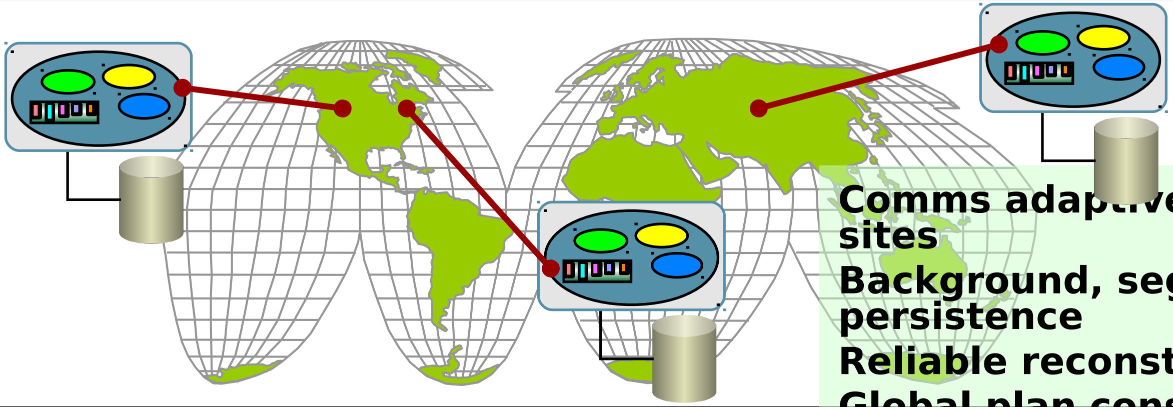
Cougaar Component Model



Internal trust models provide component-level confidence

Robust Resource-Aware Agents

Shadow key nodes in removed geographic locations



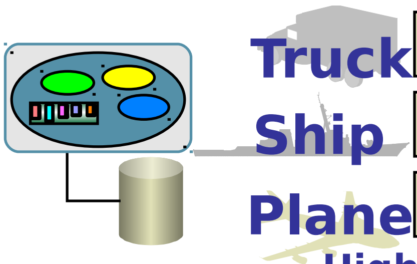
Comms adaptive shadow sites

Background, segmented persistence

Reliable reconstitution

Global plan consistency

Manage priorities & fidelity based on context specific temporal horizons



Truck	Near	Mid	Far	Future
Ship	Near	Mid	Far	Future
Plane	Near	Mid	Far	Future

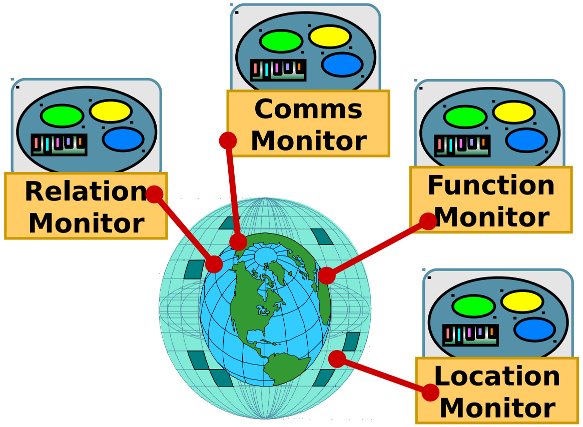
High Priority / High Fidelity

Low Priority / Low Fideli

Reconfigure clusters based on ...

Fault Tolerance

Independently survivable communities under both info and kinetic warfare

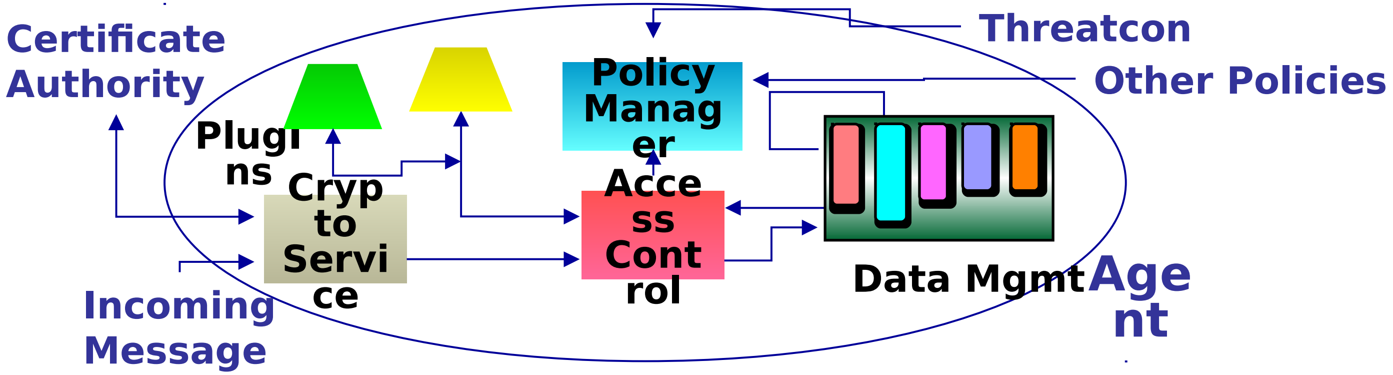


- ➘ Changing functional requirements
- ➘ Migration of functionality to user / data
- ➘ Changing information flows based on comms availability
- ➘ Dynamically changing relationships / roles

Secure Available Agents

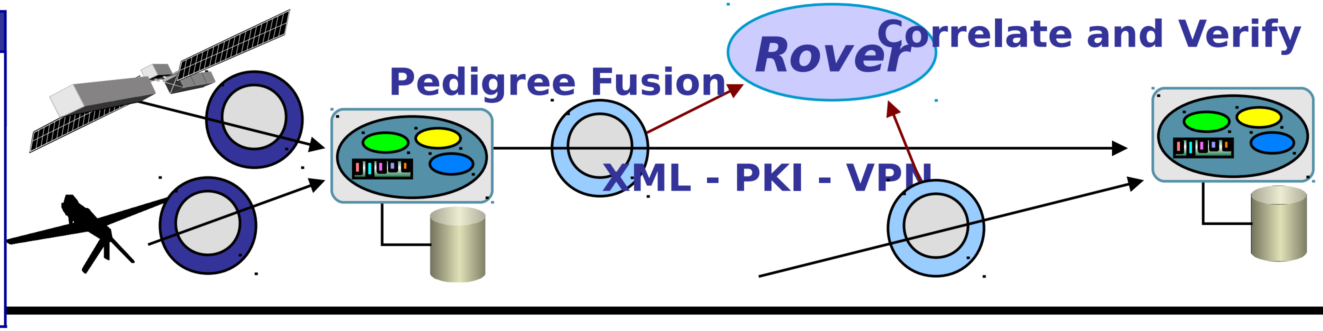
Dynamic Security

Dynamic security policy based on Threatcon & local conditions



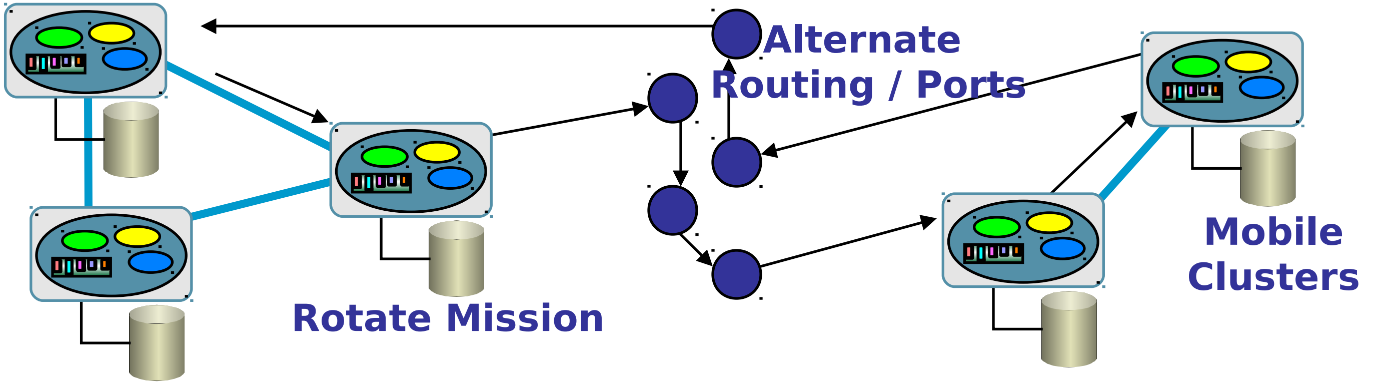
Information

Architecture level management/use of information pedigree



Adaptive Availability

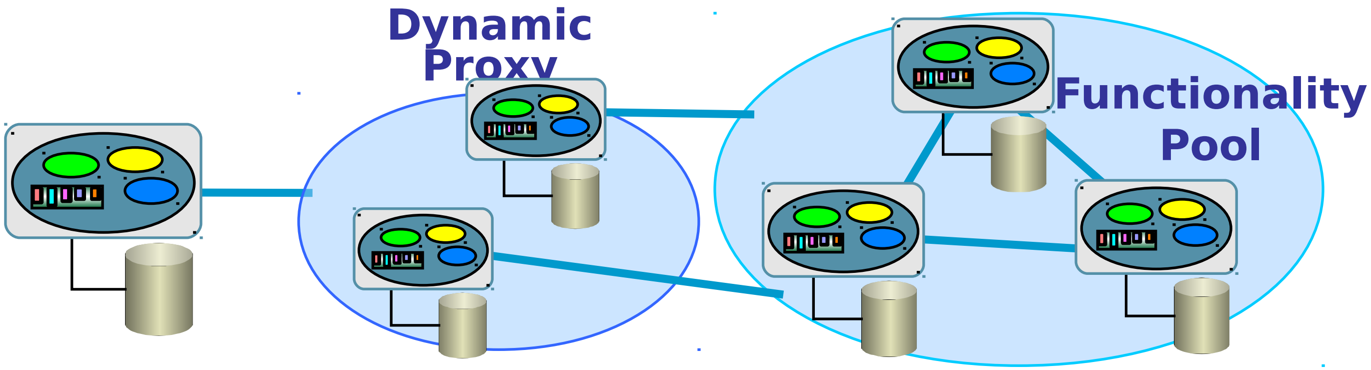
Routine and proactive reconfiguration to thwart system modeling



Scalable Agents

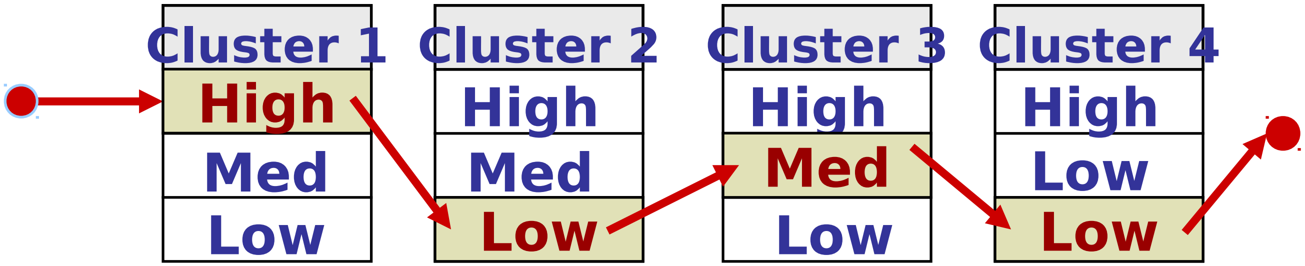
Resource

Manage high volume of intense tasks as resource pools



Variable

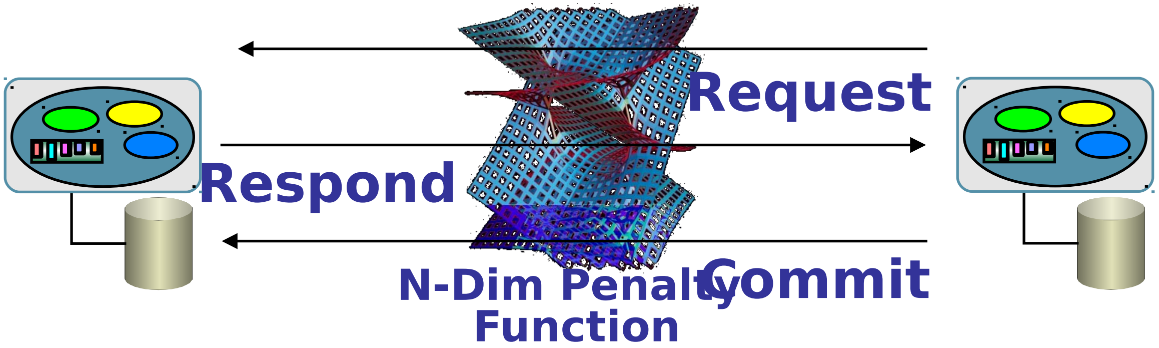
Use adaptive fidelity as proxy functions to manage comms/system requirements



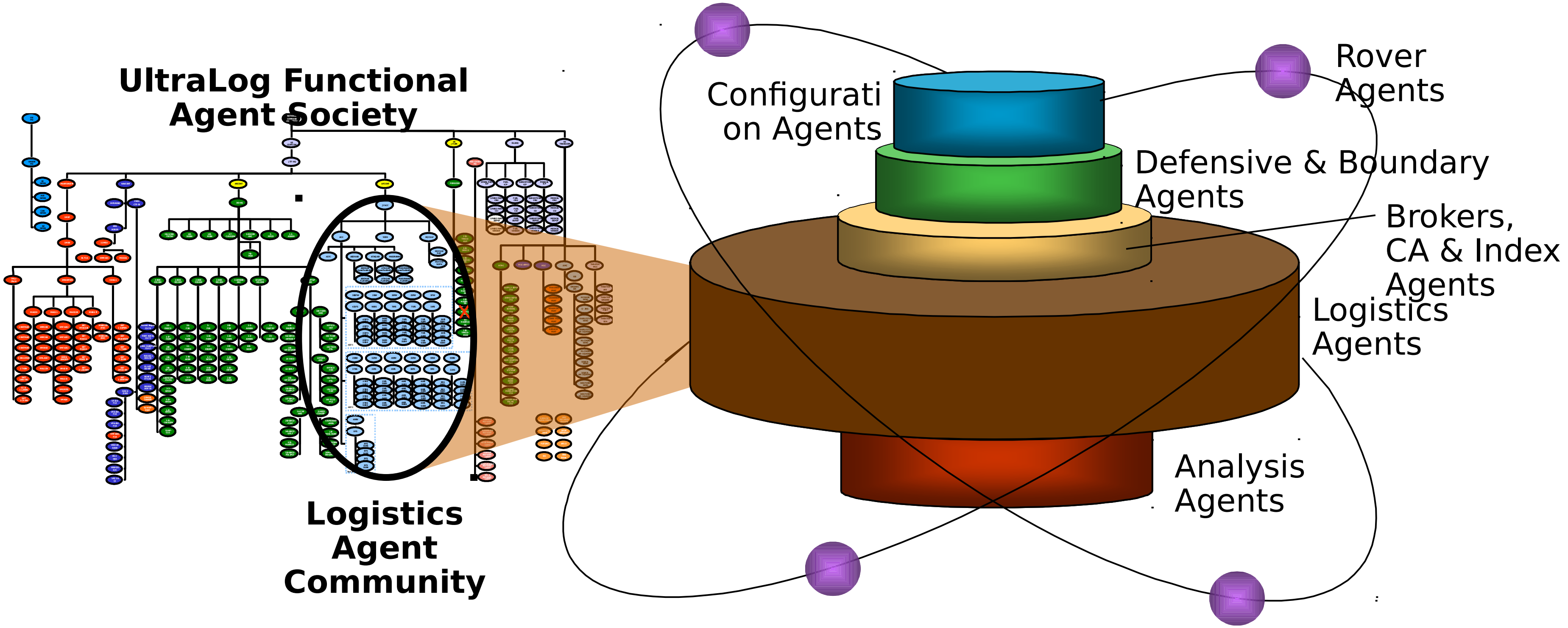
Cluster 1	Cluster 2	Cluster 3	Cluster 4
High	High	High	High
Med	Med	Med	Low
Low	Low	Low	Low

Streamlined

Negotiate information compression through complex penalty functions



Survivable Agent Communities



UltraLog Functional Agent Society

Logistics Agent Community

Configuration Agents

Rover Agents

Defensive & Boundary Agents

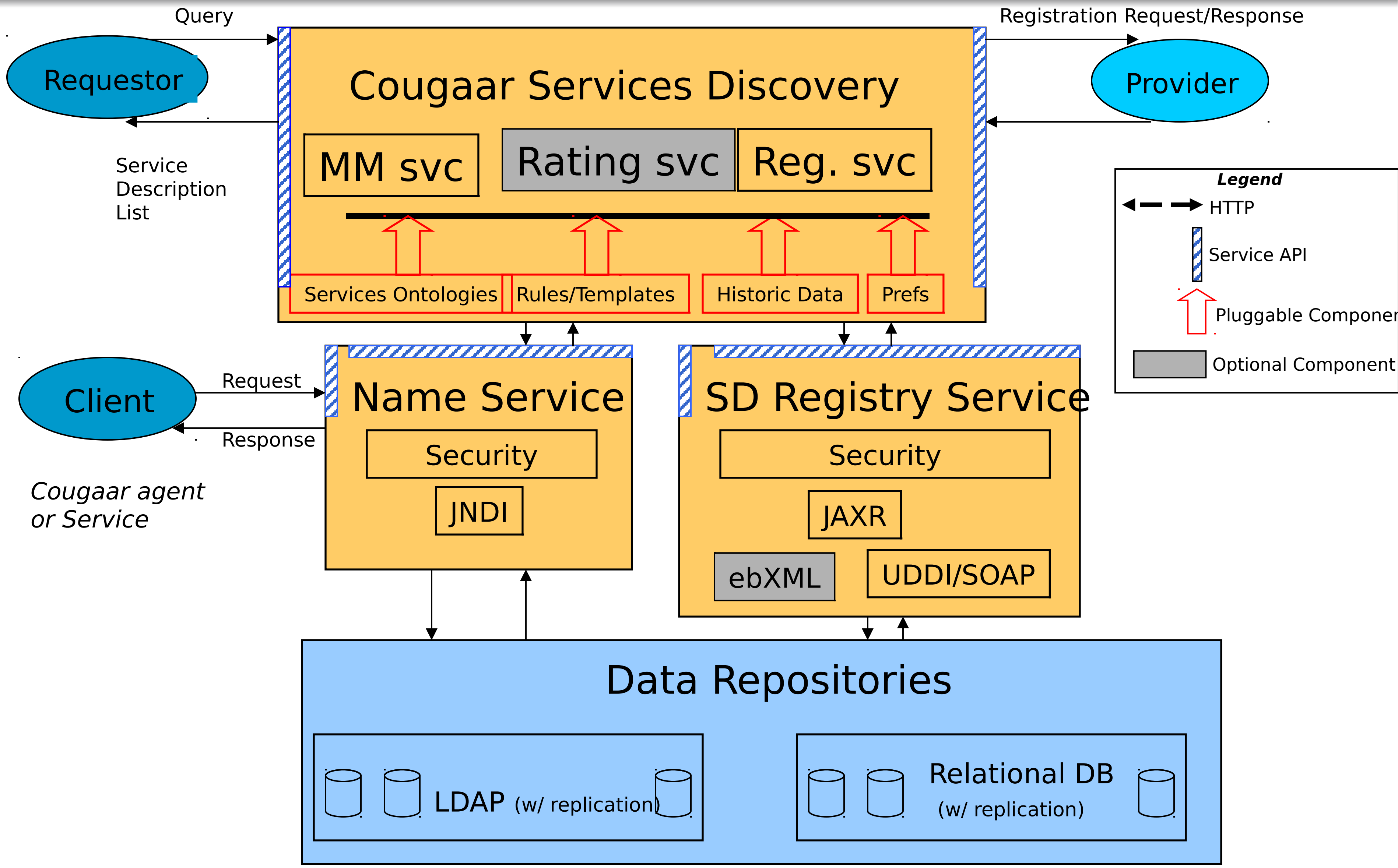
Brokers, CA & Index Agents

Logistics Agents

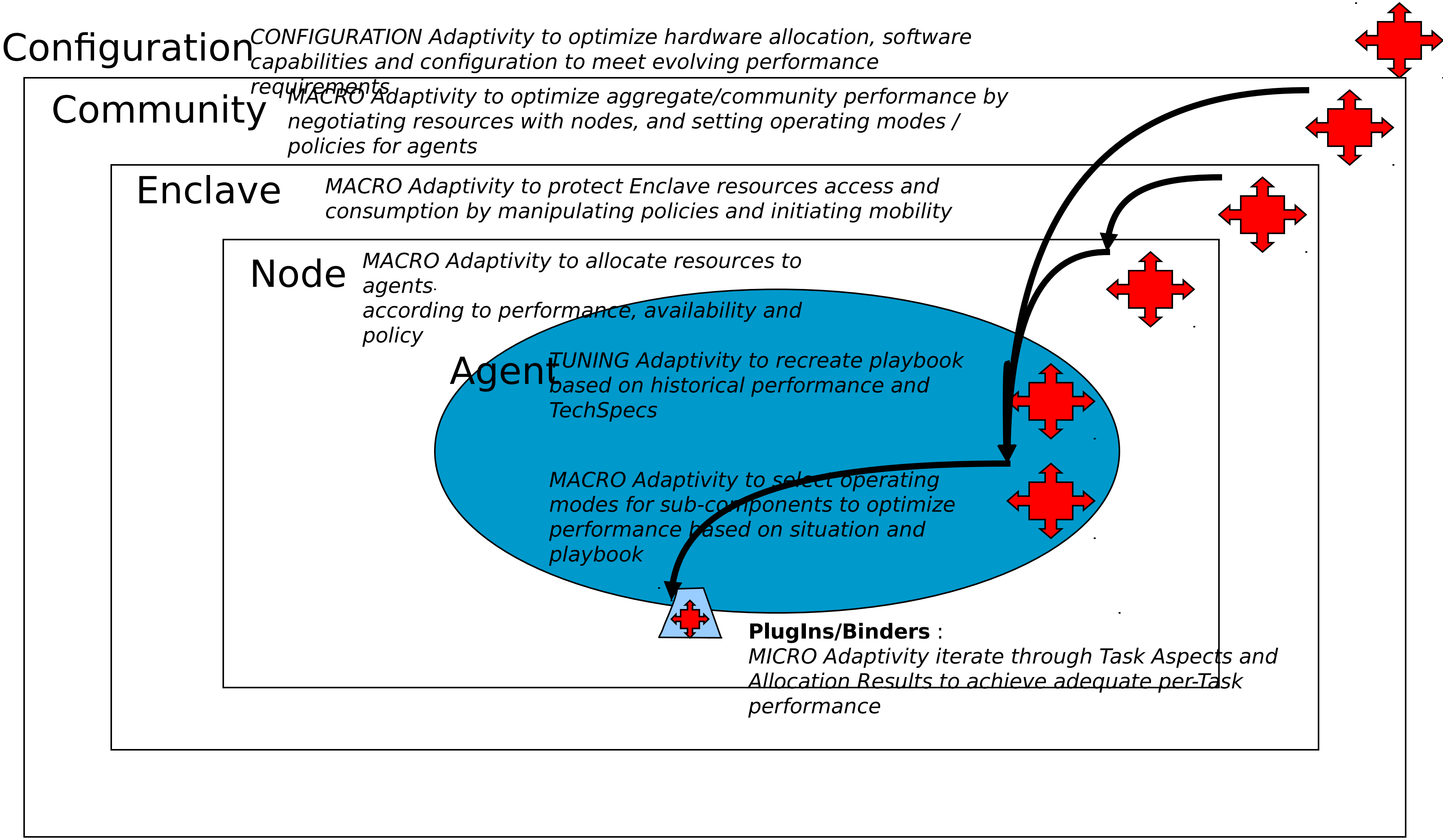
Analysis Agents

- **Survivable at all levels**
  - Overlapping communities related by functional and QoS contracts
  - Managed temporal and logical inconsistency between communities
  - Tractable policy and service conflict resolution by DAML / JTP
  - First level locus of survivability control and policy enforcement

Distributed Service Discovery



Adaptivity Engine : 2002 Scope



Configuration

CONFIGURATION Adaptivity to optimize hardware allocation, software capabilities and configuration to meet evolving performance requirements

Community

MACRO Adaptivity to optimize aggregate/community performance by negotiating resources with nodes, and setting operating modes / policies for agents

Enclave

MACRO Adaptivity to protect Enclave resources access and consumption by manipulating policies and initiating mobility

Node

MACRO Adaptivity to allocate resources to agents
according to performance, availability and policy

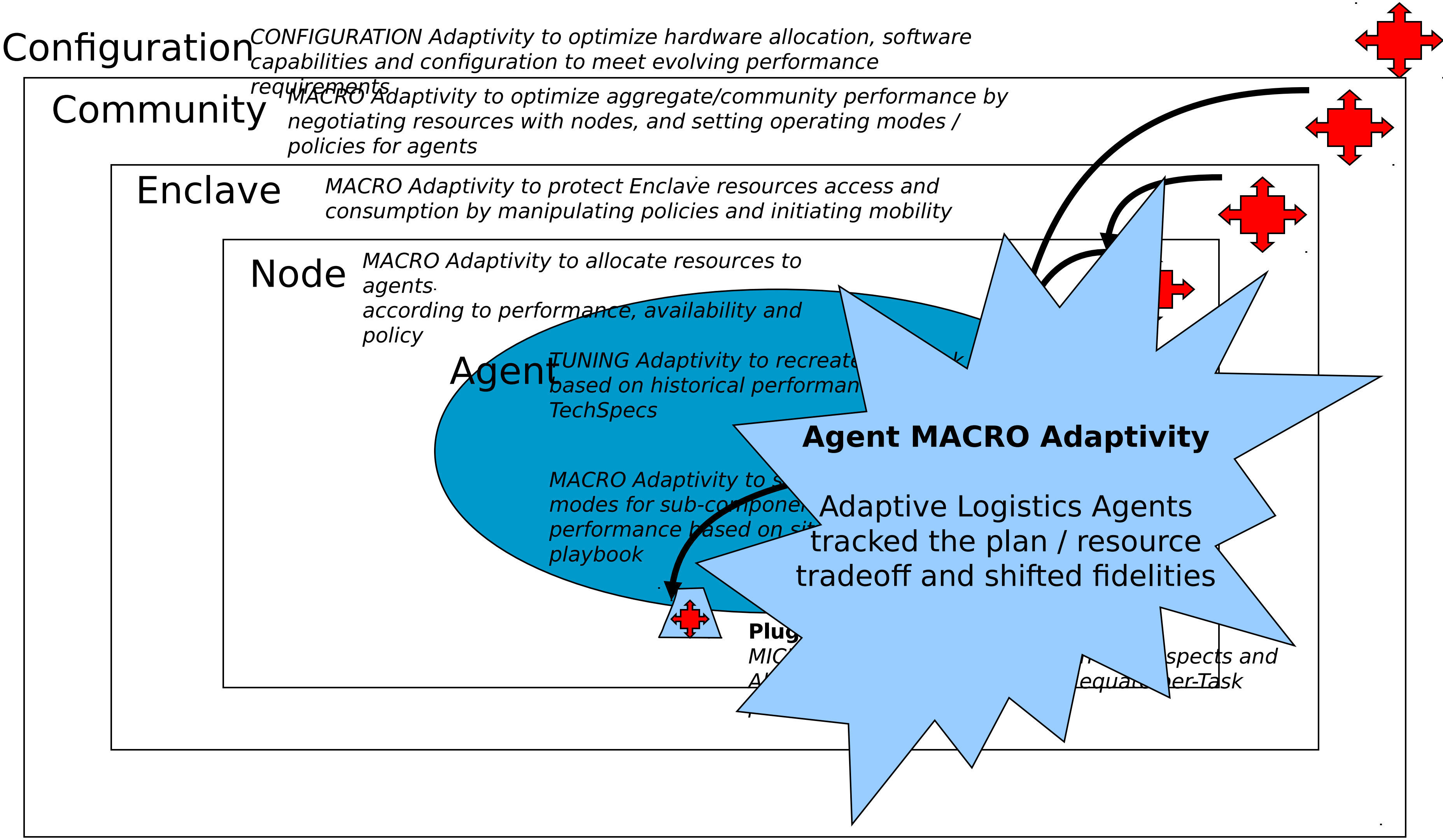
Agent

TUNING Adaptivity to recreate playbook based on historical performance and TechSpecs

MACRO Adaptivity to select operating modes for sub-components to optimize performance based on situation and playbook

PlugIns/Binders :
MICRO Adaptivity iterate through Task Aspects and Allocation Results to achieve adequate per-Task performance

Adaptivity Engine : 2002 Scope



Configuration *CONFIGURATION Adaptivity to optimize hardware allocation, software capabilities and configuration to meet evolving performance requirements*

Community *MACRO Adaptivity to optimize aggregate/community performance by negotiating resources with nodes, and setting operating modes / policies for agents*

Enclave *MACRO Adaptivity to protect Enclave resources access and consumption by manipulating policies and initiating mobility*

Node *MACRO Adaptivity to allocate resources to agents according to performance, availability and policy*

Agent *TUNING Adaptivity to recreate k based on historical performan TechSpecs*

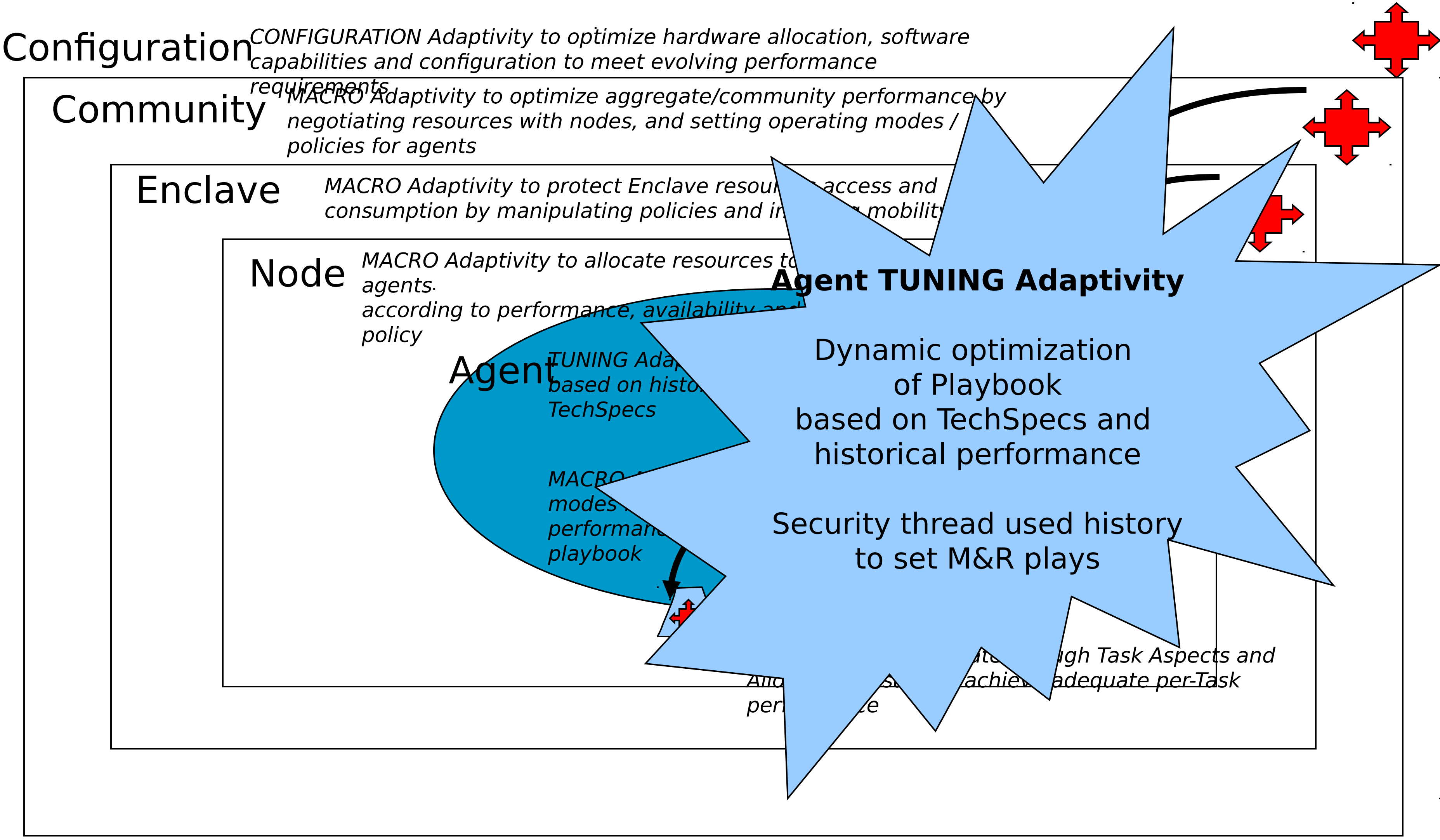
MACRO Adaptivity to s modes for sub-componen performance based on sit playbook

Plug
MIC spects and
A equat er-Task

Agent MACRO Adaptivity

Adaptive Logistics Agents tracked the plan / resource tradeoff and shifted fidelities

Adaptivity Engine : 2002 Scope



Configuration
CONFIGURATION Adaptivity to optimize hardware allocation, software capabilities and configuration to meet evolving performance requirements

Community
MACRO Adaptivity to optimize aggregate/community performance by negotiating resources with nodes, and setting operating modes / policies for agents

Enclave
MACRO Adaptivity to protect Enclave resou access and consumption by manipulating policies and in mobility

Node
MACRO Adaptivity to allocate resources to agents
according to performance, availability and
policy

Agent
TUNING Ada
based on histo
TechSpecs

MACRO
modes
performan
playbook

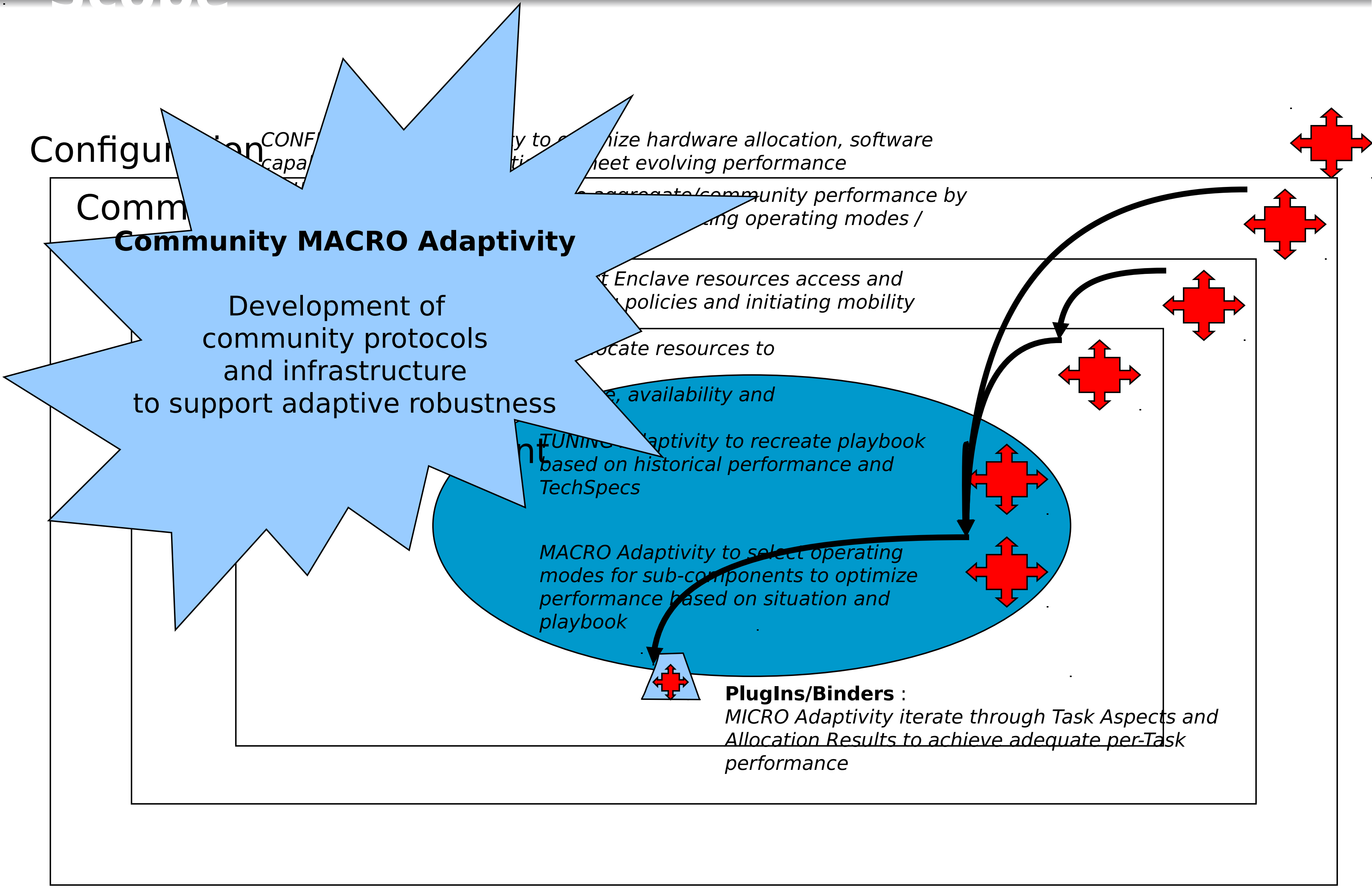
ugh Task Aspects and
Allo achie adequate per-Task
per ce

Agent TUNING Adaptivity

Dynamic optimization of Playbook based on TechSpecs and historical performance

Security thread used history to set M&R plays

Adaptivity Engine : 2002 Scope



Configur on
CONF y to o nize hardware allocation, software
capa ti eet evolving performance
Comm
aggregate/community performance by
ing operating modes /
t Enclave resources access and
policies and initiating mobility
ocate resources to
e, availability and
nt

Community MACRO Adaptivity

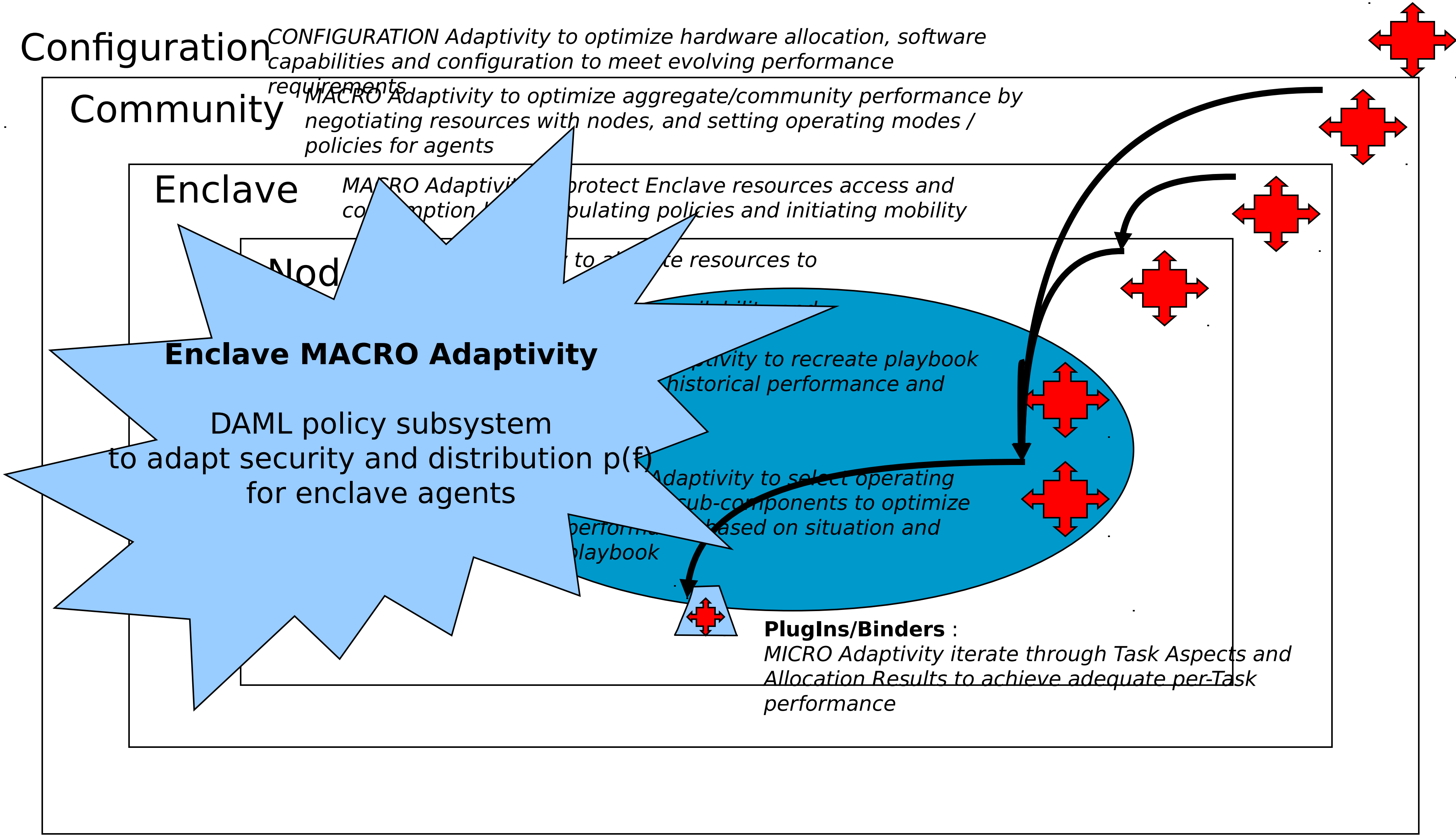
Development of community protocols and infrastructure to support adaptive robustness

TUNING aptivity to recreate playbook based on historical performance and TechSpecs

MACRO Adaptivity to select operating modes for sub-components to optimize performance based on situation and playbook

PlugIns/Binders :
MICRO Adaptivity iterate through Task Aspects and Allocation Results to achieve adequate per-Task performance

Adaptivity Engine : 2002 Scope



Configuration *CONFIGURATION Adaptivity to optimize hardware allocation, software capabilities and configuration to meet evolving performance requirements*

Community *MACRO Adaptivity to optimize aggregate/community performance by negotiating resources with nodes, and setting operating modes / policies for agents*

Enclave *MA RO Adaptivi protect Enclave resources access and co mption ulating policies and initiating mobility*

Nod *y to al te resources to*

ptivity to recreate playbook historical performance and

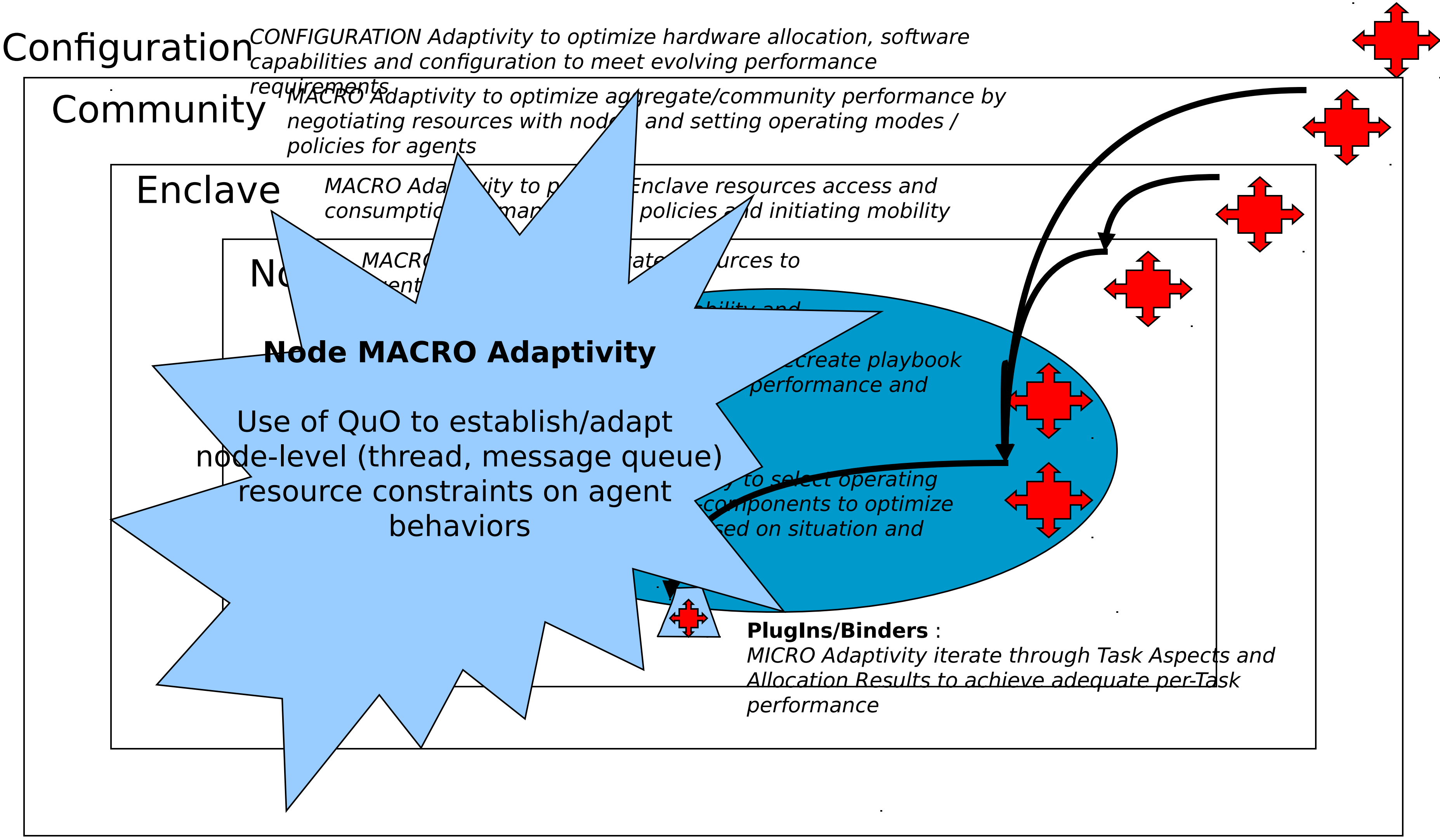
Adaptivity to select operating sub-components to optimize performa based on situation and playbook

Enclave MACRO Adaptivity

DAML policy subsystem
to adapt security and distribution p(f)
for enclave agents

PlugIns/Binders :
MICRO Adaptivity iterate through Task Aspects and Allocation Results to achieve adequate per-Task performance

Adaptivity Engine : 2002 Scope



Configuration

CONFIGURATION Adaptivity to optimize hardware allocation, software capabilities and configuration to meet evolving performance requirements

Community

MACRO Adaptivity to optimize aggregate/community performance by negotiating resources with nod and setting operating modes / policies for agents

Enclave

MACRO Ada ity to p Enclave resources access and consumptio man policies and initiating mobility

No

MACRO ate urces to ent

bility and

create playbook performance and

to select operating components to optimize sed on situation and

Node MACRO Adaptivity

Use of QuO to establish/adapt node-level (thread, message queue) resource constraints on agent behaviors

PlugIns/Binders :
MICRO Adaptivity iterate through Task Aspects and Allocation Results to achieve adequate per-Task performance

2002 Survivability Infrastructure of Cougaar

- Security
  - Encryption
    - Message Transport, Messaging, Naming Service
    - Data Protection Service to encrypt persistence data
  - Certificates
    - Certificates for agents, user authentication; CA management, CRLs, Mobility
    - Unified user/agent security model with roles, permissions, attributes
  - Java Security Model, JAAS
  - Rovers for spot checks
  - DAML policy subsystem for role-based permissions and obligations
- Reliable and Incremental Persistence
  - Persists local agent information on distributed BFS file system
  - Fast reconciliation between agents resolving asymmetries
  - Backup for entire system not necessary
- Agent Mobility
  - Provides directives that dynamically move an agent from one host to another
  - DISA-compliant Level 2 mobile code

2002 Survivability Infrastructure of Cougaar

- Management Agents
  - Observe and control defined portions of the agent society
- Distributed Sensor Network
  - Provides QoS metrics … ping, bandwidth, etc
  - Fully adaptive messaging framework
- Agent Restart
  - Automatic detection and restart of crashed agents
  - Detects DOS attacks and automatically starts counter measures (dynamic defenses)
- Load Balancing
  - Automatic, dynamic optimization of agent topology (agent to host distribution) using online sensor data and agent move directives
- Adaptivity engines and basic playbook syntax
  - Adaptivity at agent, node, enclave, and community
  - Resource-aware logistics agents

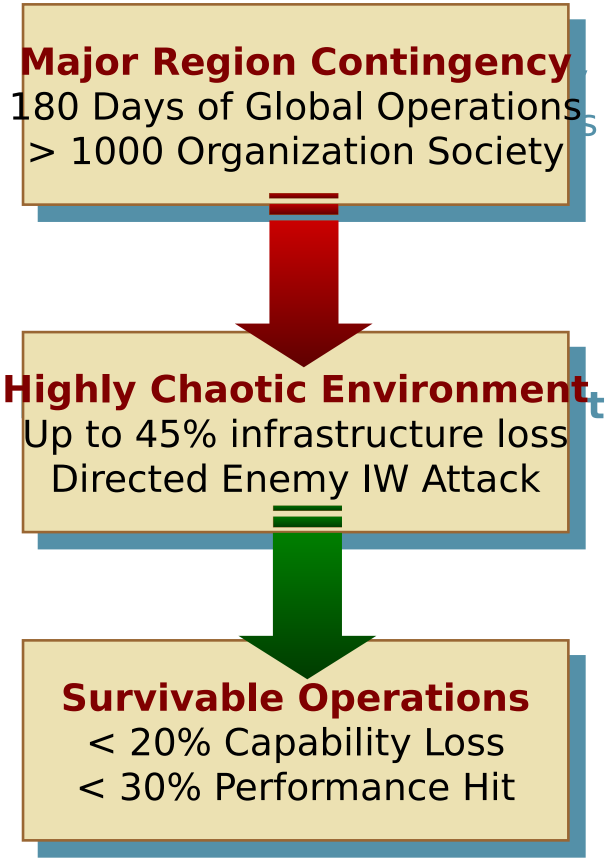
Questions

Metrics for Survivability

UltraLog Survivability Claim

UltraLog will act to maximally preserve society function under stress, in accordance with policy

- ***Function*** **is defined by requirements**
  - Measures of Effectiveness, Operational Issues, Measures of Performance, Data Requirements, and the MAU score
  - UltraLog has both Logistics MOPs and Security MOPs
- ***Stress*** **is defined by the UltraLog program goals and threat environment**
  - Define Security, Scalability, Robustness stresses
  - Apply stresses singly, per-class, and jointly, in accordance with the experimentation plan
- ***Policy*** **supplies a set of tradeoff constraints**
  - Security policies provide minimum levels of integrity and confidentiality
  - Functional policies constrain the logistics solution
- ***Act to maximally preserve*** **means the generation, optimization, and application of UltraLog control strategies**
  - Define sensors, actuators, state estimators
  - Construct system control laws and strategies



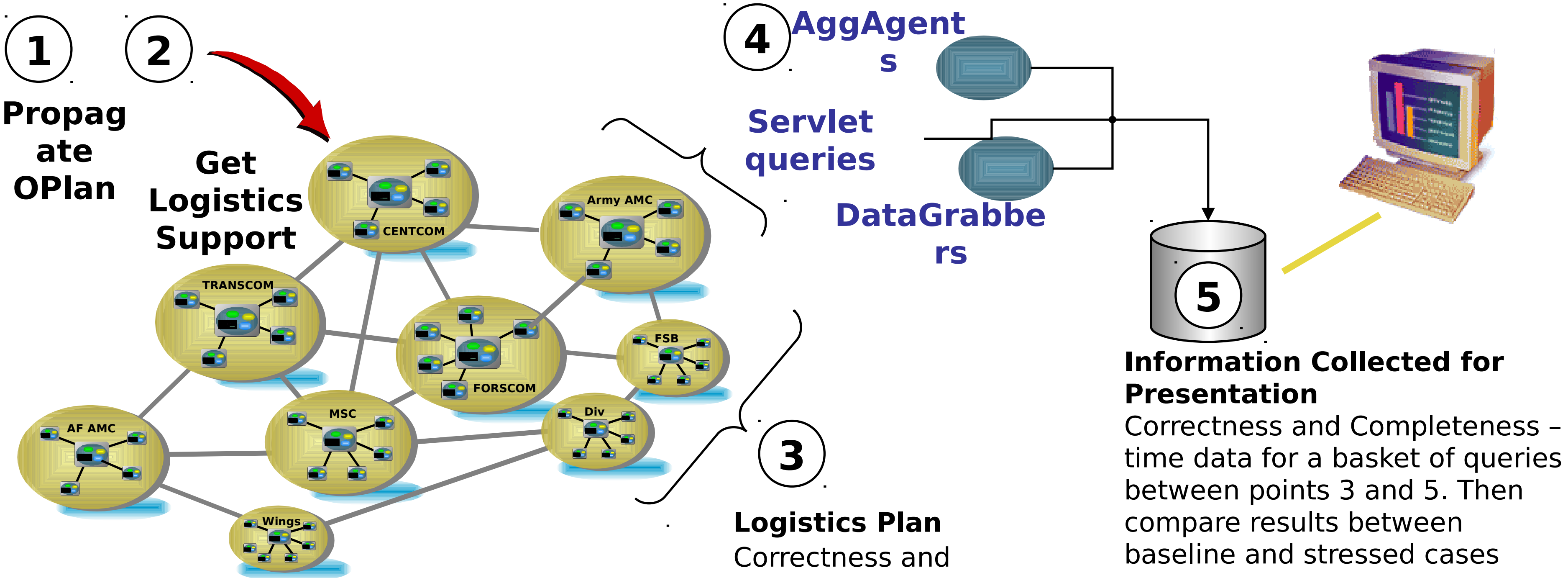
Major Region Contingency
180 Days of Global Operations
> 1000 Organization Society

Highly Chaotic Environment
Up to 45% infrastructure loss
Directed Enemy IW Attack

Survivable Operations
< 20% Capability Loss
< 30% Performance Hit

Measures of Performance

Correctness, Completeness and



1 Propagate OPlan

2 Get Logistics Support

4 AggAgents

Servlet queries

DataGrabbers

3 **Logistics Plan**

Correctness and Completeness – measure allocation results for root tasks at point 3 and compare baseline and stressed cases

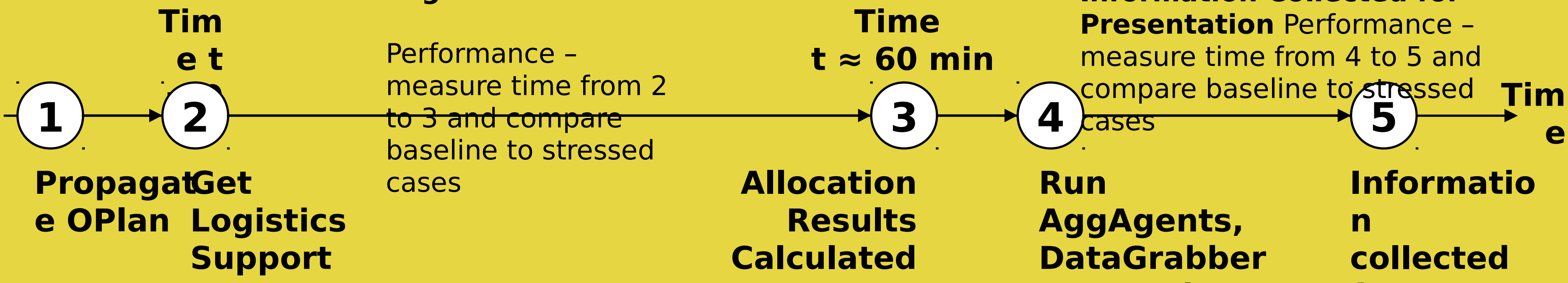
5 **Information Collected for Presentation**

Correctness and Completeness – time data for a basket of queries between points 3 and 5. Then compare results between baseline and stressed cases

Log Plan Generation

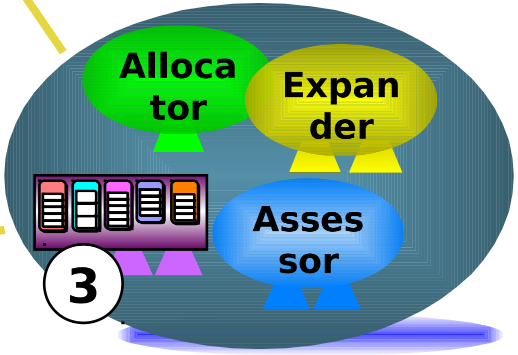
Performance – measure time from 2 to 3 and compare baseline to stressed cases

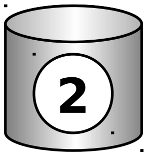
Information Collected for Presentation Performance – measure time from 4 to 5 and compare baseline to stressed cases



Measures of Performance
Confidentiality and Accountability

1 **Accountability of User Actions**
a. Measure percentage of user actions that were available for invocation counter to authorization policy and effort required to invoke them
b. Measure percentage of user actions that were not recorded and effort required prevent it

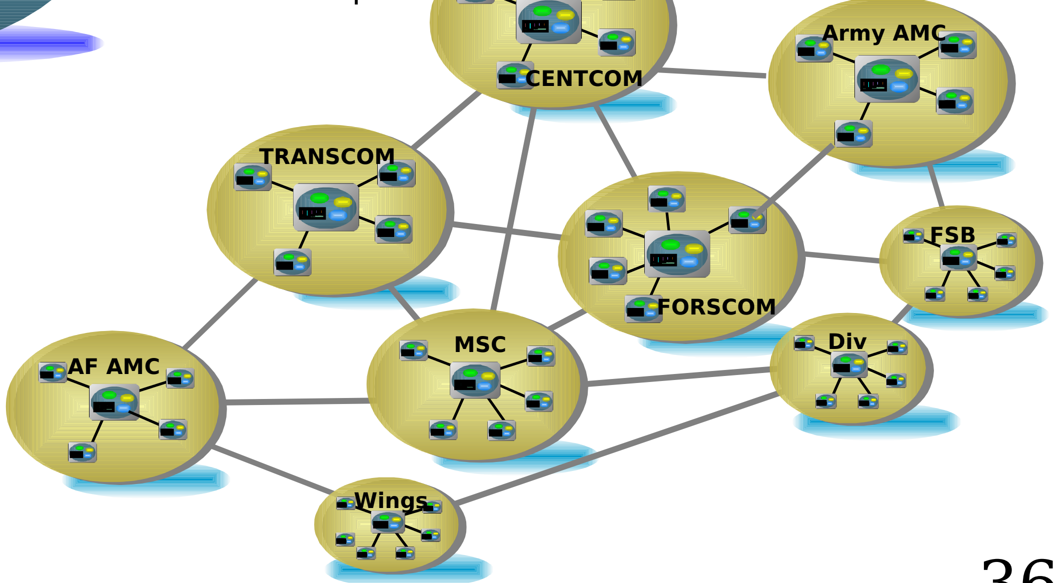




Confidentiality of Data in Storage
Measure percentage of data elements available to unauthorized entity and effort required to disclose it

Confidentiality of Data in Memory
Measure percentage of data elements available to unauthorized entity and effort required to disclose it

4 **Confidentiality of Data in Transit**
Measure percentage of data elements available to unauthorized entity and effort required to disclose it



Recent UltraLog Successes

- In a 185-agent UltraLog society:
  - Planning speed increased by 4x over ALP
    - Level 5 TPFDD for SSC in 15 minutes from OPLAN entry
    - Better schedulers and inventory managers, use of multiple fidelities and sliding time windows, more parallelism
  - Verified continued operations under kinetic attack
    - Simultaneous failure of 40% of UltraLog society agents
    - Failure was detected, new resources allocated, functionality restored
    - Recovery from denial of service attacks demonstrated
  - Two complete Red Team assaults on UltraLog by SNL / IDART
    - Found and corrected numerous security holes
    - Implemented IMDEF-compliant monitoring system for commercial interoperability
    - Third Red Team assault in December 02
  - Full mobility
    - All agents can change hosts at any time and in any phase, with no loss of functionality, allowing for “scram” scenarios.
- Collection of 2002 Assessment Data is happening right now

Backup Slides

Programmatics

UltraLog's Focus in 2002

- **2002: Survivability of the Society**
  - 2001 gave a nice basket of components, but fairly little overall improvement in survivability (except security)
  - Further development of capabilities needed to be coordinated
- **Defense Threads**
  - Shift from individual survivability components to end-to-end reactive capability to stresses
  - Teams of developers to focus on particular stress threads
    - Prepare technical approach
    - Develop components for avoidance, containment, detection, recovery
    - Develop control flows, "glue," and integration
    - Include members of integration team, ISAT team, and assessment team
  - Threads are about survivability claims. Each thread makes a claim about how to best handle a specific type of stress
  - Threads are Robustness/FT; Scalability; Adaptive Security; Adaptive Logistics
  - Support threads are TIC Infrastructure, Open Source, DLA SD

UltraLog Transition Plan

Department of Defense

Defense Logistics Agency

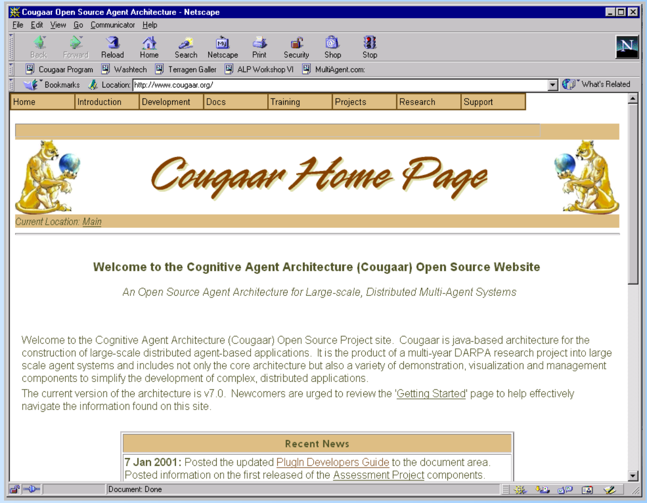
Future Combat System

Global Combat Support System

Focused Logistics Wargame

UltraLog
& Cougaar

Open Source


Cougaar Open Source Agent Architecture - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Cougaar Program Washtech Terragen Galler ALP Workshop VI MultiAgent.com:
Bookmarks Location: http://www.cougaar.org/ What's Related
Home Introduction Development Docs Training Projects Research Support
Document: Done

Cougaar Home Page

Current Location: Main

Welcome to the Cognitive Agent Architecture (Cougaar) Open Source Website

An Open Source Agent Architecture for Large-scale, Distributed Multi-Agent Systems

Welcome to the Cognitive Agent Architecture (Cougaar) Open Source Project site. Cougaar is java-based architecture for the construction of large-scale distributed agent-based applications. It is the product of a multi-year DARPA research project into large scale agent systems and includes not only the core architecture but also a variety of demonstration, visualization and management components to simplify the development of complex, distributed applications.

The current version of the architecture is v7.0. Newcomers are urged to review the 'Getting Started' page to help effectively navigate the information found on this site.

Recent News

7 Jan 2001: Posted the updated PlugIn Developers Guide to the document area. Posted information on the first released of the Assessment Project components.

www.cougaar.org

Open Source License

Commercial transitions

Free training classes

UltraLog Program Schedule

Developer Team

- NAI, BBN, Boeing, SRA, LMI, MIC, OBJS, PSU, MIC, 21st Century, IHMC, UMemphis, Honeywell, Stanford

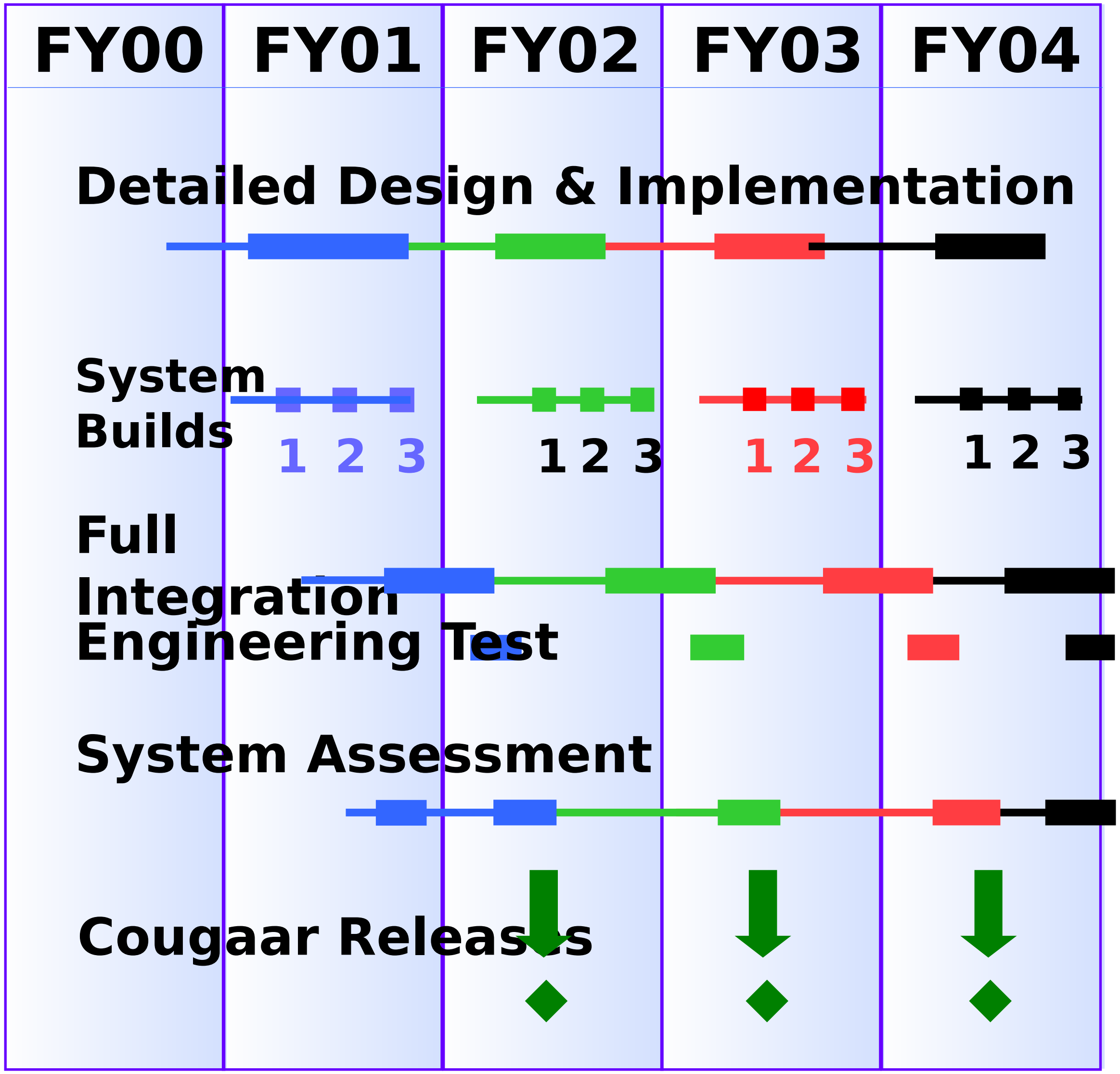
Integration Team

- BBN, Lockheed-Martin, InfoEther

Assessment Team

- SRI, LATA, Sandia, LMI

CCB Transition



FY00 FY01 FY02 FY03 FY04

Detailed Design & Implementation

System Builds

Full Integration

Engineering Test

System Assessment

Cougaar Releases

UltraLog’s End Products

General Architecture and Specific Algorithms For Survivable Agent Systems

- Revolutionary software for survivability
  - Secure, scalable, and robust network-centric logistics infrastructure
    - Enable precision logistics at high tempos
    - Survivability in the electronic battlefield
  - Extensions to survivable C2 infrastructures
    - Distributed C2 systems that combine high-survivability with increased speed-of-command and information quality
    - High-confidence C2

Cougaar Applications for Chaotic Environments

- Hardened Cougaar
  - Transitions using DARPA’s Cougaar Open Source base
  - New Cougaar applications for highly demanding conditions
- Reliable control of the logistics pipeline
  - Absorb cyber attacks and massive infrastructure loss with controlled degradation and robust failover
  - Scale to multiple operations and global sizes

UltraLog will demonstrate that agent technology is ***dependable*** in the harshest wartime environments

Conclusion: Transforming Logistics

ALP: Integrated Logistics

- Generated a level 5 TPFDD for an SSC in less than an hour
- Planned and monitored execution of multiple simultaneous operations
- Dynamically replanned as problems and changes occurred

UltraLog: Survivable Logistics

- Software agents that create a logistics capability that reliable and dependable even in the harshest and most chaotic wartime environments
- Controlled degradation of logistics function when under stress

Greater user-level logistics confidence with reduced stockages and better overall flow management

Tailored logistics support for the complete operational spectrum

Survivability for the modern information battlefield

ransformational technology for Focused Logist

Backup Slides

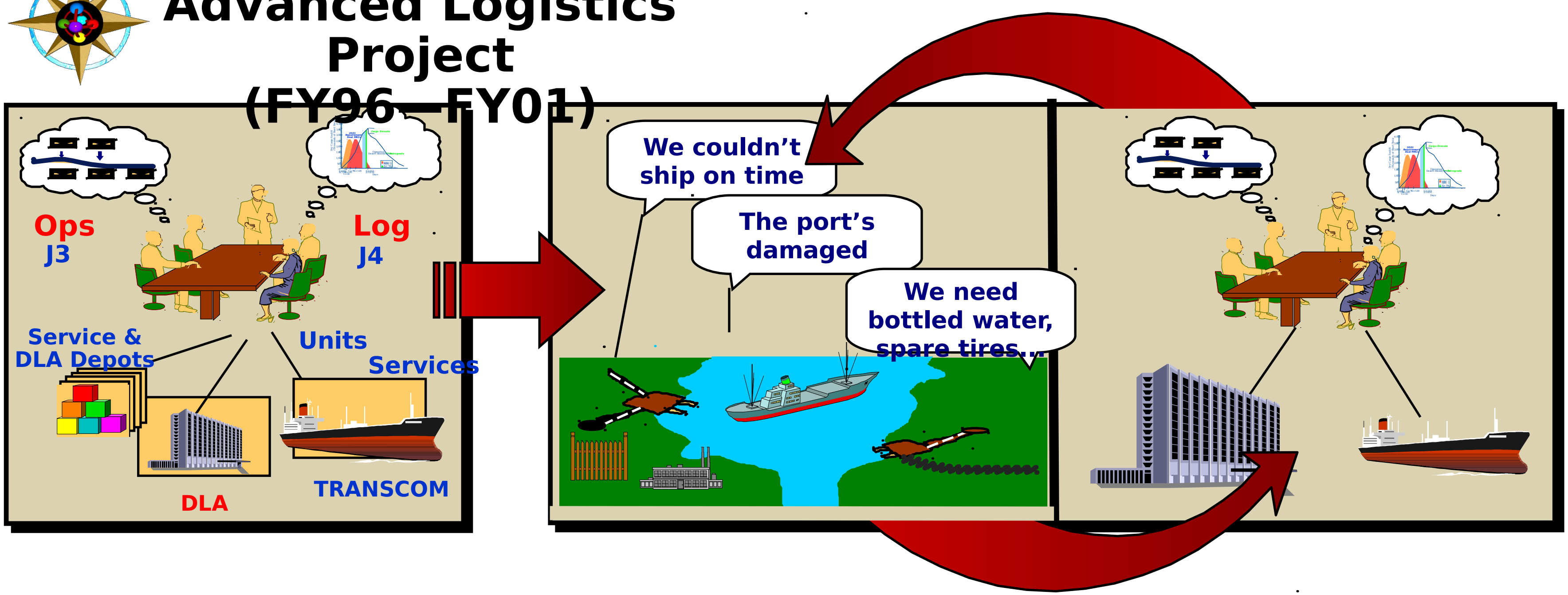
Backup Slides

Backup Slides

Why Agents for Logistics?

Focused Logistics Vision

Advanced Logistics Project (FY96—FY01)



Rapid Planning

- All Echelons
- Executable detail
- Globally optimize

Execution Monitoring

- Manage flow
- Deploy plan sentinels
- Localize problems

Continuous Replanning

- Redirected flow
- Localized Replanning
- Locally optimal fixes

Continuous Dynamic Planning, Monitoring and Replanning

Joint Vision 2020: Focused Logistics Pillar

- World-wide time definite delivery
- Assured, real time situational awareness/ information
- Single point of contact for customer service
- Logistics response; not inventory
- Smaller logistics footprint
- Less cost for support & services
- Confidence in delivery of right items, right time, right place, right price, every time

Network-centric Logistics

020 goals rely on the precise, reliable, and timely fus
ution of vast amounts of physically distributed logisti

Classic Logistics Systems

- Characteristics
  - Centralized data warehouses with long-reach data feeds
  - Tightly integrated database and applications
  - Centralized control of business processes and relationships
- Benefits
  - Well understood model
  - Very mature technology
- Issues
  - Scaling of data rates
  - Best for static organizations and processes

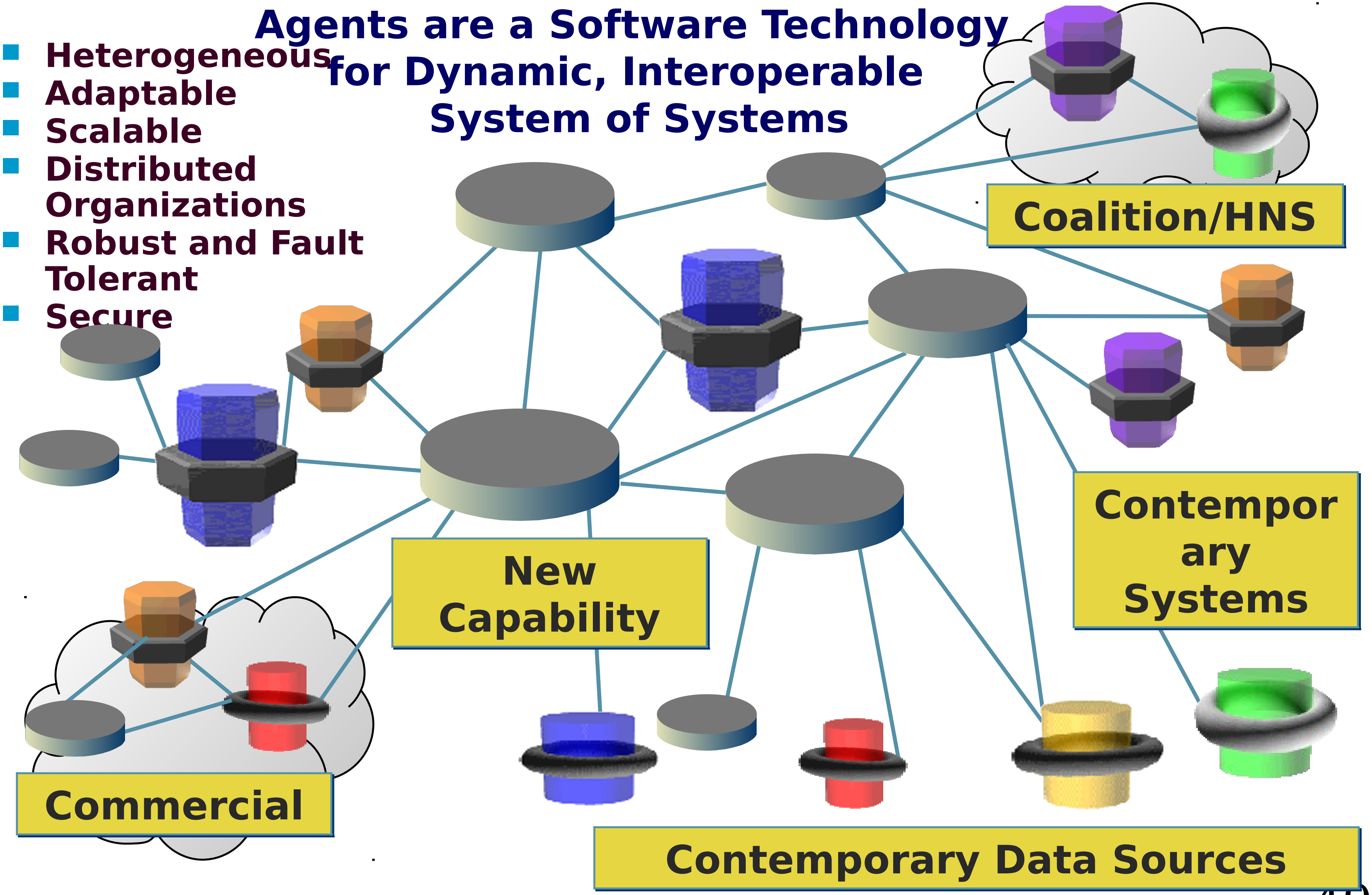
Network-centric Logistics

- Characteristics
  - Data and business processes distributed throughout the enterprise
  - Local data fusion with drill-down capability
- Benefits
  - Adapts well to dynamic collaborative supply chains
  - More robust, scalable, reliable
  - Easy to evolve for different business processes
  - Highly customer focused
- Issues
  - Requires new kinds of software

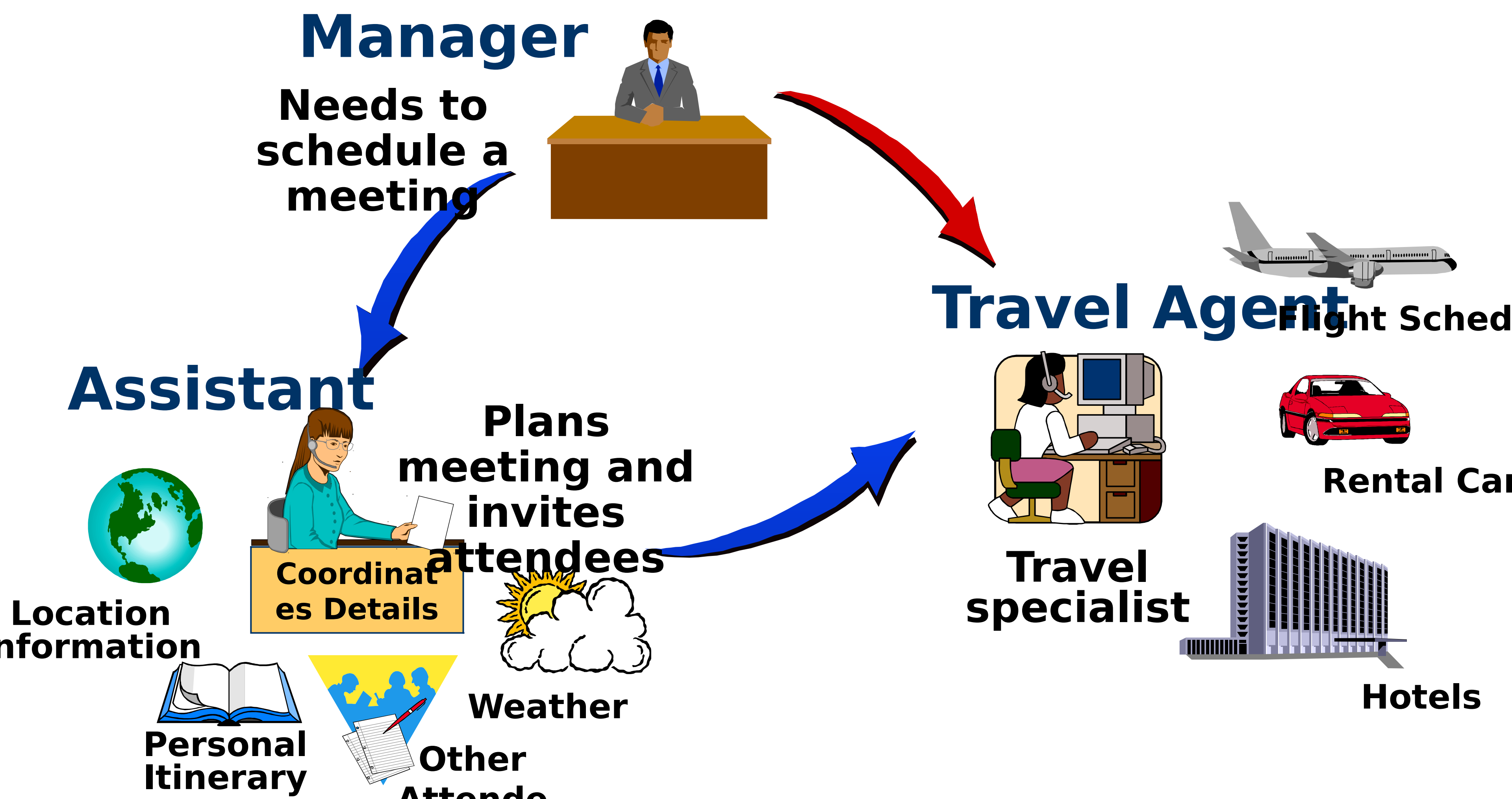
Agents Enable Systems of Systems

- Heterogeneous
- Adaptable
- Scalable
- Distributed Organizations
- Robust and Fault Tolerant
- Secure

Agents are a Software Technology for Dynamic, Interoperable System of Systems



Concept of an Agent



Manager

Needs to schedule a meeting

Travel Agent

Flight Sched

Rental Car

Travel specialist

Hotels

Assistant

Plans meeting and invites attendees

Coordinates Details

Location nformation

Personal Itinerary

Other Attendees

Weather

An independent person or entity that can autonomously accomplish tasks for another person or other entity

What is a Software Agent?

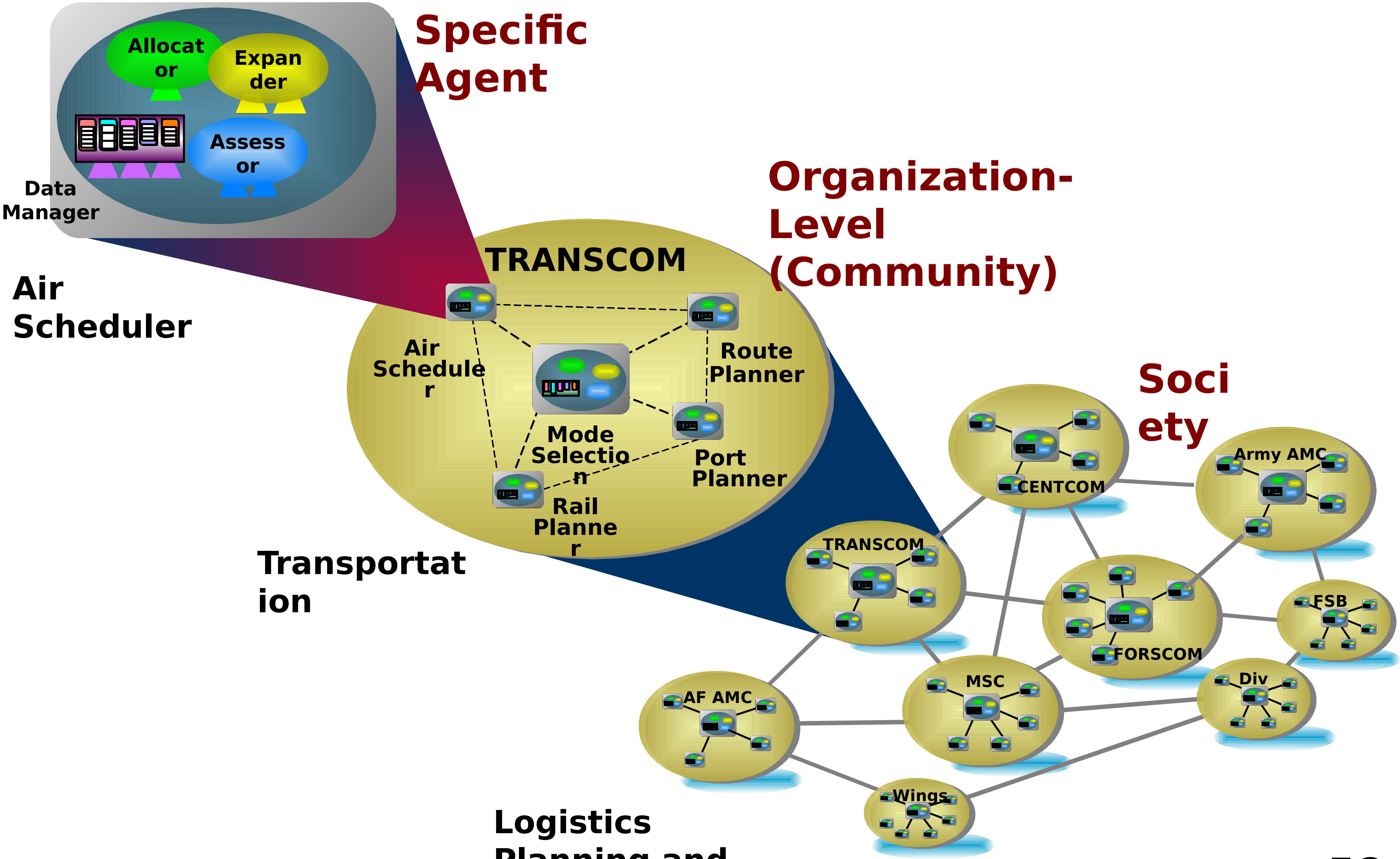
- Agents are software pieces that autonomously accomplish tasks on behalf of another entity
- Agents are a style of computer program
  - They execute as machine code just like all other programs
  - They are not magic; just because you program

    solved very hard AI problems

Typical Properties of Software Agents

- **Goal Oriented and Taskable**
- **Autonomous**
- **Collaborative**
- **Adaptive**
- **Proactive**
- **Extensible**
- **Mobile**

Using Agents to Construct a Net-Centric Logistics Information



Domain Specific Agent

Organization-Level (Community)

Society

Air Scheduler

Transportation

Logistics Planning and

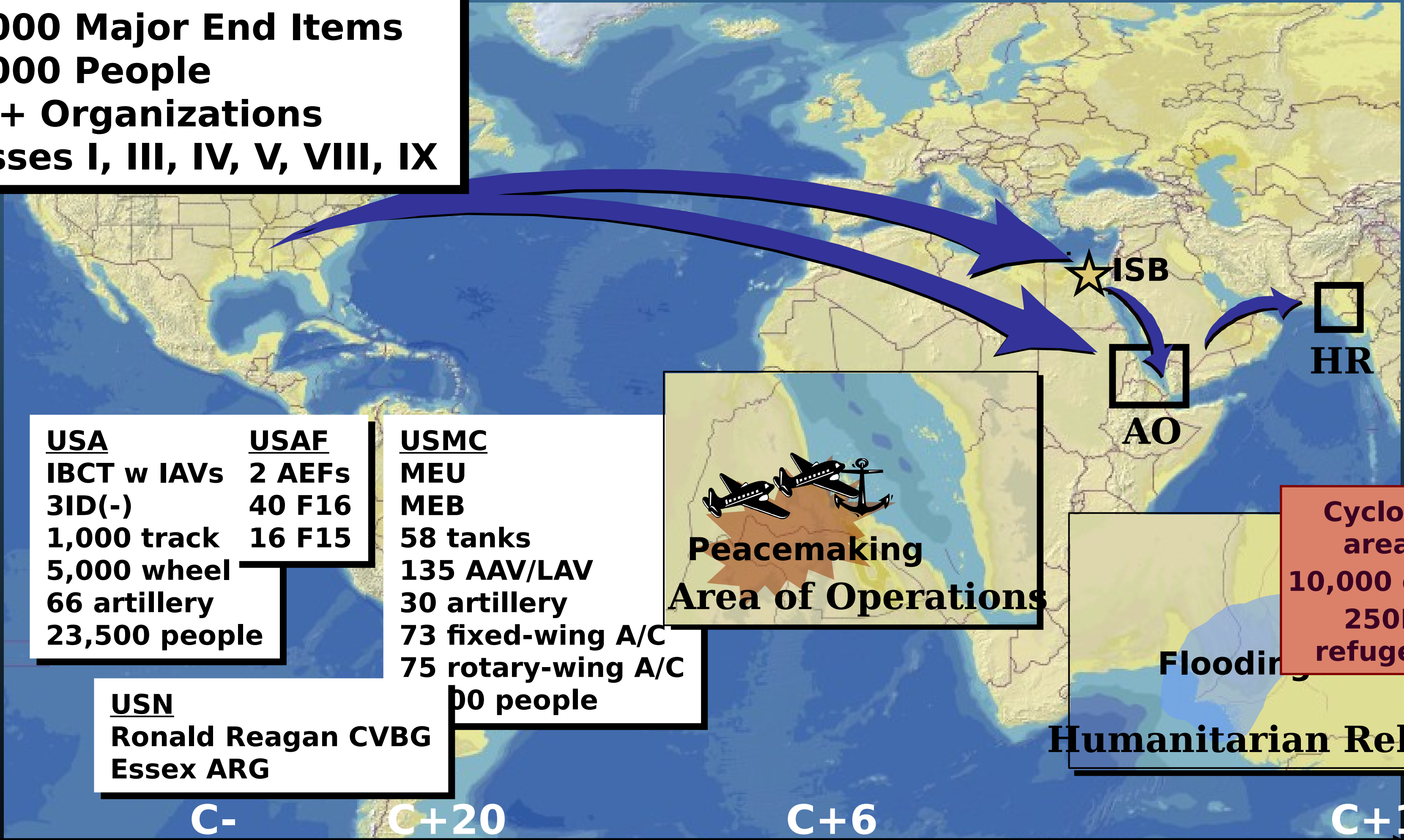
ALP Final Functional Demonstration

May 2001

ULTRALOG

5,150 Business Processes
20,000 Major End Items
33,000 People
300+ Organizations
Classes I, III, IV, V, VIII, IX

Hypothetical 2005 Force Deployme



USA
IBCT w IAVs
3ID(-)
1,000 track
5,000 wheel
66 artillery
23,500 people

USAF
2 AEFs
40 F16
16 F15

USMC
MEU
MEB
58 tanks
135 AAV/LAV
30 artillery
73 fixed-wing A/C
75 rotary-wing A/C
00 people

USN
Ronald Reagan CVBG
Essex ARG

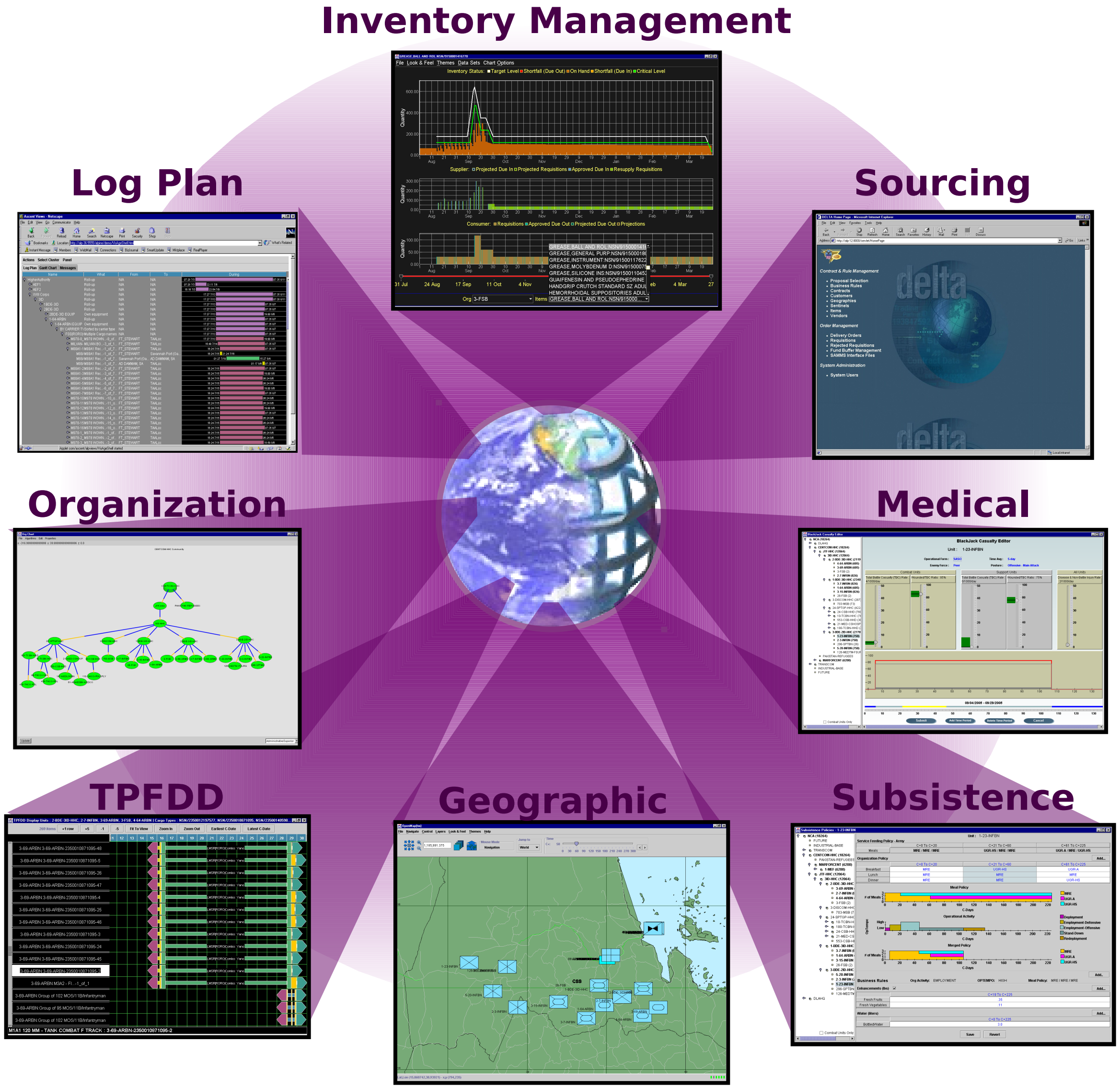
Cyclone area:
10,000 dead
250K refugees

C- C+20 C+6 C+18

SSC | Pre | Deploy ment | Peace Making | Peace Keeping

Aug 15 | Sep 4 | HR | Nov 4 | Transition/Redepl

Logistics Functionality



Elements of The Plan

- 300 orgs, 33,000 people, 20,000 MEIs
- 4 services, DLA, TRANSCOM
- HNS, NGOs, Coalition Forces
- Transportation Fort to In-Theater Dest classes I, III, IV, V, VIII, IX
- Time-Phased demand/sourcing
- DS/GS Maint, Material Handling,
- ISB Transshipment
- 3-echelon medical care
- ... and much more

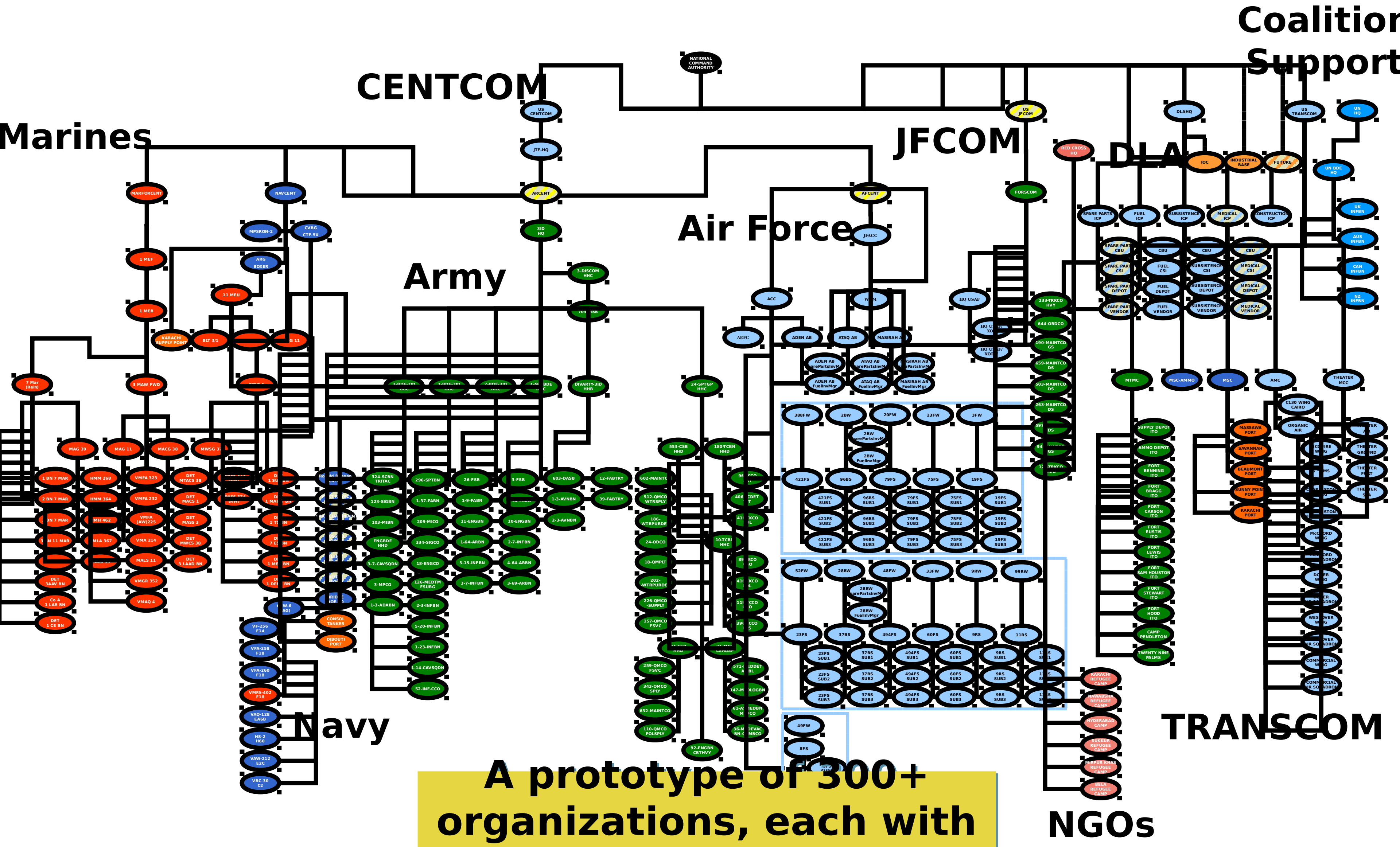
Elements of The Demo

- Execution Monitoring
- Dynamic Replanning
- Multiple concurrent operations
- Live Business Rule Changes

Elements of The Society

- 300+ agents, 30 machines
- Standard NT/Linux machines
- Web based displays, Local

World’s Most Complex Agent Society



A prototype of 300+ organizations, each with one or more agents.

Development of the Log Plan

2 Course of Action

Passed @ t=0

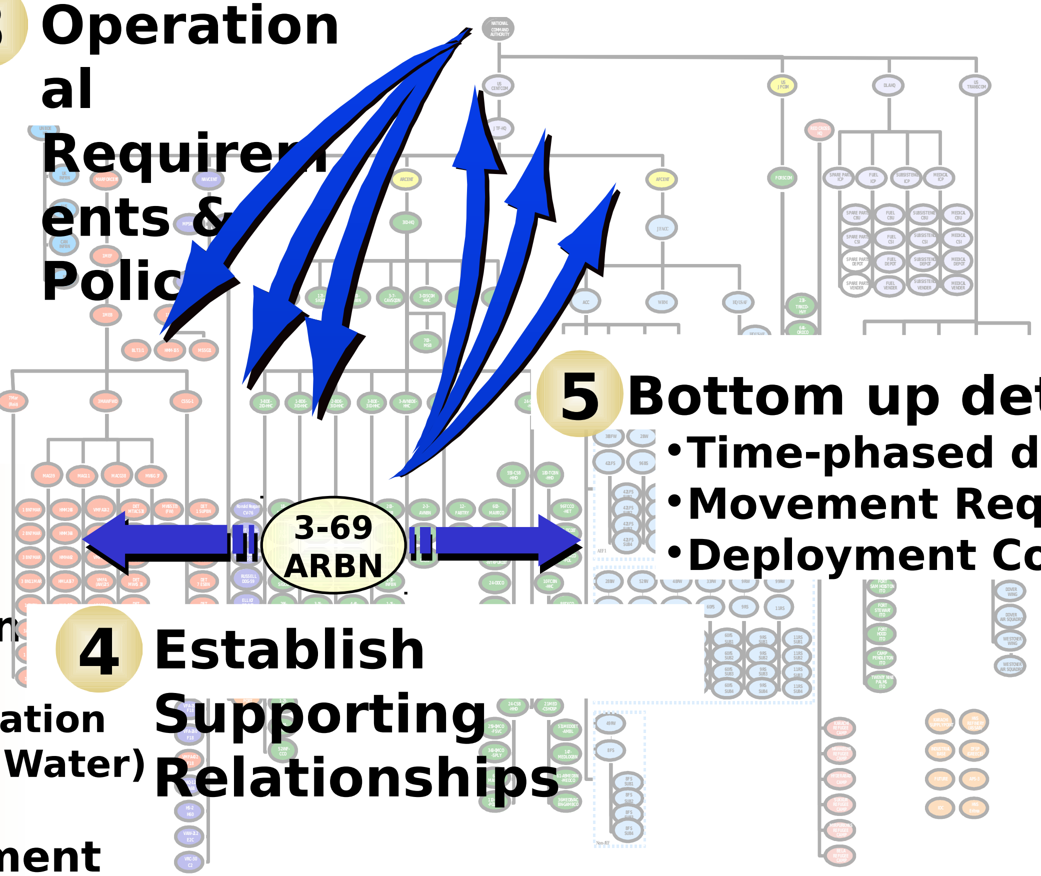
Time Phased Mission Requirements

Op Tempo

- Mission Activity
- Location Requirements (RDD, EAD, etc.)

Log Plan Develop

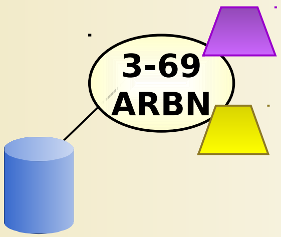
3 Operational Requirements & Polic



5 Bottom up detai

- Time-phased dem
- Movement Requir
- Deployment Cons

1 Data & PlugIns



JTAV, TCAIMS II

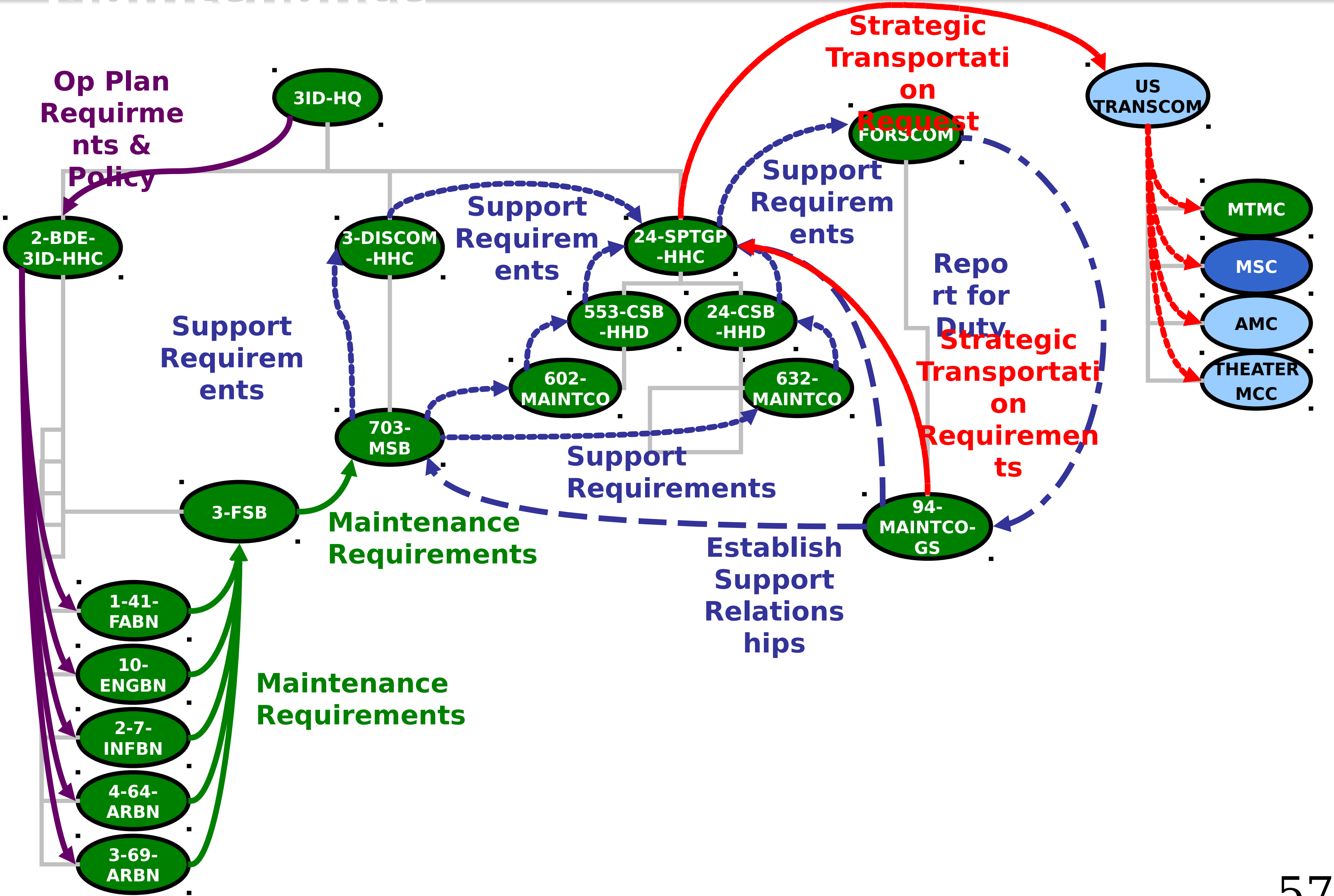
Demand Generation

- Supply
- Strategic Transportation
- Subsistence (Food, Water)
- Major End Items

Inventory Management

4 Establish Supporting Relationships

Example Thread: Maintenance



UltraLog Products

Cougaar

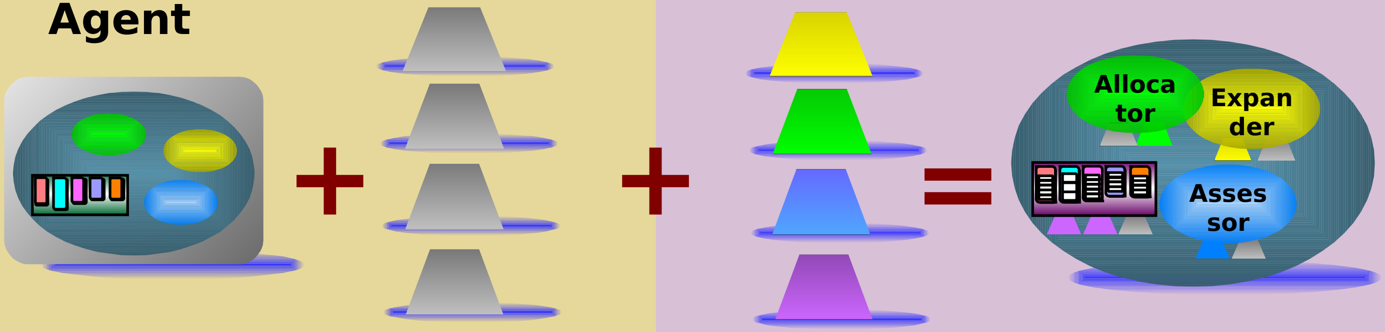
UltraLog Society

Generic Agent

Generic PlugIns

Specific PlugIns

Domain Agent



- Basic building blocks
- Easy to specialize
- Domain independent

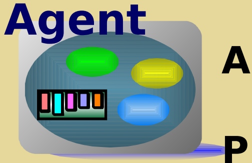
- Military specific processes
- Interfaces to military systems
- Specific to Logistics Domain

Cougaar : Cognitive Agent Architecture

ALP Products

Cougaar

Generic Agent

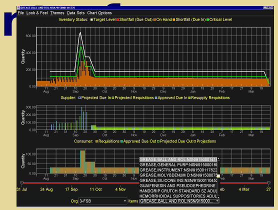


Architecture Document
PlugIn Developer Guide

Generic PlugIns

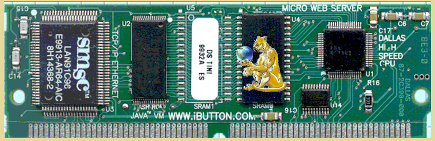
Scheduler
Assessor
Inventory Management
Skills based Personnel Management
Demand Generation
Sourcing

Generic User In



Inventory Viewer
Map Viewer
Organizational Viewer
Assessment Viewer

Micro Edition



Sensor Web
Robotics

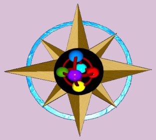
Actuators
Sensors

Tools

Three Tier UI Framework
Scalability Tester
Configuration Management
Dynamic Configuration
Contracts Base Management
CSMART

Training

Basic Course
Advanced Course

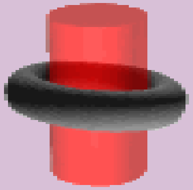


ALP Prototype

Military Specific PlugIns

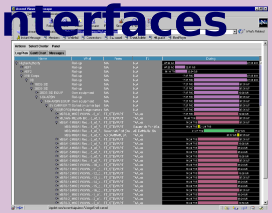
Scheduler (sea, air, overland, rail, ISB Transshipment)
Skills based Personnel Management (Army DS/GS Maintenance)
Demand Generation (I,III,V,VII,VIII,IX)
Sourcing (I,III,V,VII,VIII,IX)

Wrappers & Interfaces



TCAIMS II, GTN, JTAV
SAMMS, POPS, MOMS
World Wide Port System
ULLS
etc. …

Military User Interfaces



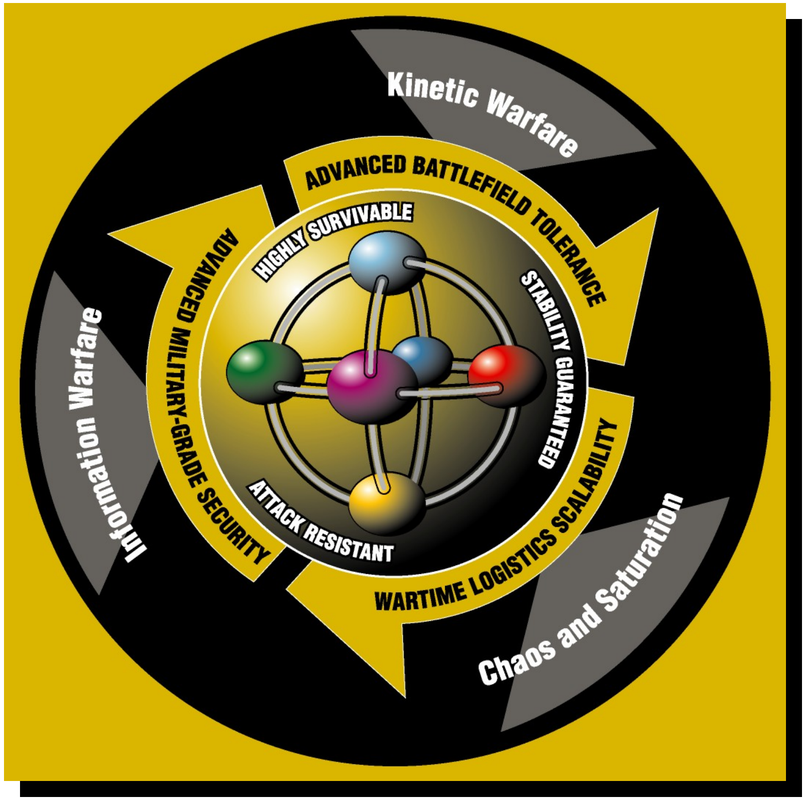
TPFDD Viewer
Medical Demand Views
DELTA Viewer
Subsistence

Backup Slides

UltraLog Details

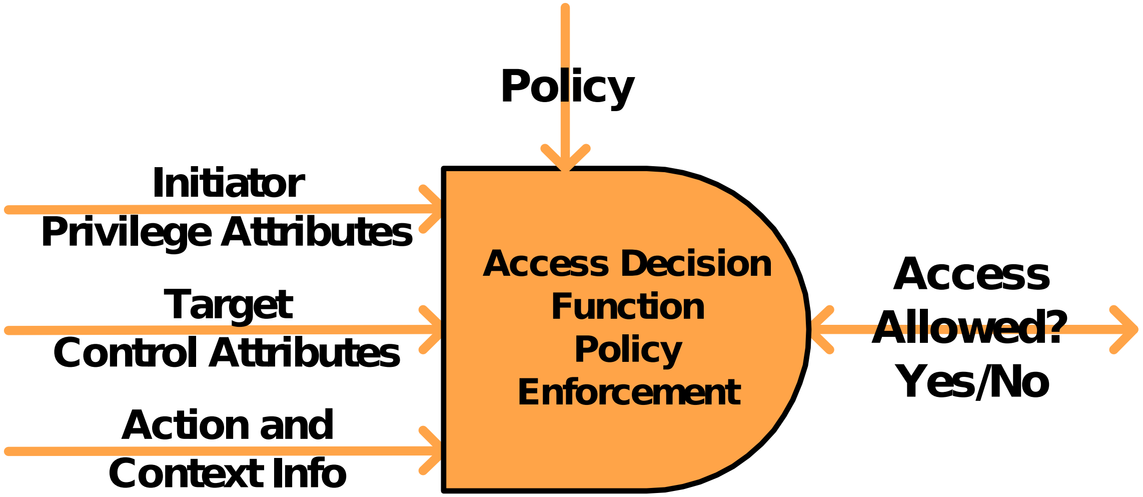
Approaches to Survivability

- **A survivable information system**
  - Demonstrate continuity of operations while under extreme stress
  - Build on a sophisticated agent workflow framework
- **A strategy for technical success**
  - Treat survivability as an derivative property
  - Develop a distributed agent-based interoperable system of systems, providing:
    - *Security* – Protect confidentiality and integrity of data and resources
    - *Robustness* – Resist, contain, and recover from damage
    - *Scalability* – Stable under rapid changes in size of tasks and resources
  - Assume that best practices of operating systems and network security frequently fail
  - Balance security, scalability and robustness in a continuous tradeoff
- **A strategy for software confidence**
  - Applications to DoD
  - Commercial adoption via open source model



UltraLog Security Framework:

- Includes policy definition, distribution, expansion, and enforcement
- Fundamental policy enforcement point is a *binder*
  - No component trusts any other component
  - Binders mediate all system and data access


Policy
Initiator Privilege Attributes
Target Control Attributes
Action and Context Info
Access Decision Function Policy Enforcement
Access Allowed? Yes/No

UltraLog Security Framework:

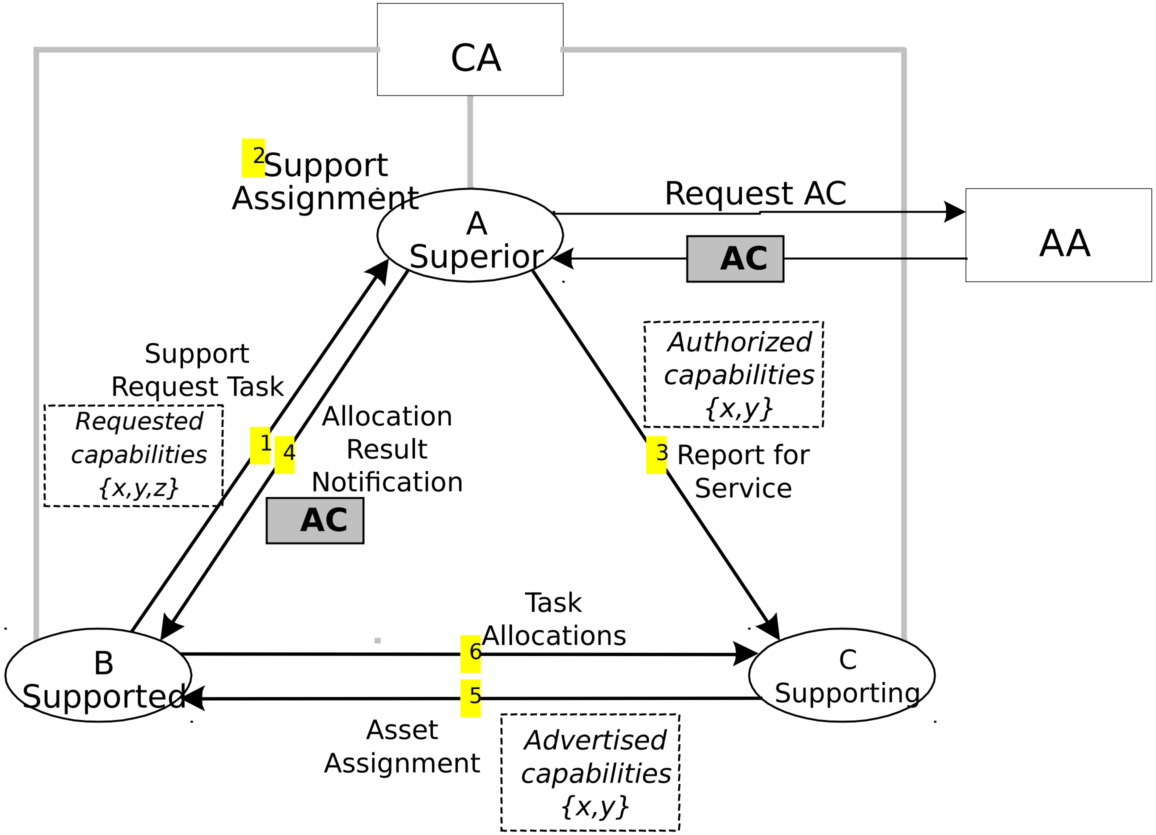
- Implemented via binders and Java mechanisms (JAAS)
- Controls and Regulates:
  - Inter-agent communication
  - Intra-agent interactions
  - Interactions with users
  - Interactions with legacy systems and external databases
- Enforces Dynamically Changing Policies
- Leverages Emerging COTS/GOTS Access Control Mechanisms (Service Providers)
- Defines a Common Interface to Service Providers

UltraLog Security Framework:

- Functional objectives
  - Provide ability to protect confidentiality and integrity of data and programs when in transit and when in storage
  - Provide means for authenticating identity of users and agents
  - Provide means for distributing rights
  - Provide strong accountability for actions by users and agents
- Implementation Services
  - Cryptographic hashing, digital signatures, attribute and identity certificate management, pluggable encryption and decryption algorithms, end-entity initialization
  - Includes commercial and DoD cryptographic algorithms
  - Experiments with biometrics and smart cards for storage of cryptographic material

Trust-based Interaction

- *B* signs message. *A* can verify originator of message using identity certificate of *B*.
- *A* creates attribute certificate for *B* granting rights to service
- *A* tells C to report for service
- *A* sends attribute certificate to *B*
- *C* reports for service to *B*
- *B* signs message and sends attribute certificate to *C*. *C* can verify that *B* has appropriate rights to allocate tasks.



UltraLog Security Framework:

- Functional objectives
  - M&R maintains a defensive posture by detecting and responding to attacks, faults, and errors
    - A defensive posture is one that can continue to support critical operations
    - Thwarting attacks
    - Eliminating points of weakness
  - Operates with minimal human intervention
  - M&R system is difficult for an attacker to exploit
  - M&R operates in an environment of limited resources
- Standards-based
  - Uses IMDEF-based M&R components